

EXHIBIT 1

Redacted in its Entirety

EXHIBIT 2
Redacted in its
Entirety

EXHIBIT 3
Redacted in its
Entirety

EXHIBIT 4
Redacted in its
Entirety

EXHIBIT 5
Redacted in its
Entirety

EXHIBIT 6

Message

From: Alexei Svitkine (Gerrit) [noreply-gerritcodereview-SAtWTFZ-2udUgWqpJhJPfA==@chromium.org]
Sent: 6/18/2021 3:23:01 PM
To: Ramin Halavati [rhalavati@chromium.org]
CC: akanchagupta@google.com; vgallet@google.com; Theresa [twellington@chromium.org]; Boris Sazonov [bsazonov@chromium.org]; Tricium [tricium-prod@appspot.gserviceaccount.com]; Chromium LUCI CQ [chromium-scoped@luci-project-accounts.iam.gserviceaccount.com]; chromium-reviews@chromium.org
Subject: Update Incognito session metrics to consider restored sessions. [chromium/src : main]

Attention is currently required from: Ramin Halavati, Theresa .

Patch set 19:Code-Review +1

[View Change](#)

1 comment:

- Patchset:
 - [Patch Set #19:](#)

Does this affect how UMA sessions show in our dashboard? [...]

My understanding from this change is it's not modifying how UMA cuts logs or anything like that and is only affecting some specific metrics around Incognito used being logged, which I'm deferring to Ramin's team as the owners.

But let me know if I'm misunderstanding and this is having some more fundamental impact on UMA.

To view, visit [change 2919846](#). To unsubscribe, or for help writing mail filters, visit [settings](#).

Gerrit-Project: chromium/src

Gerrit-Branch: main

Gerrit-Change-Id: I9746ce327af27c415deca64357b410bb06b07ebd

Gerrit-Change-Number: 2919846

Gerrit-PatchSet: 19

Gerrit-Owner: Ramin Halavati <rhalavati@chromium.org>

Gerrit-Reviewer: Alexei Svitkine <asvitkine@chromium.org>

Gerrit-Reviewer: Boris Sazonov <bsazonov@chromium.org>

Gerrit-Reviewer: Ramin Halavati <rhalavati@chromium.org>

Gerrit-Reviewer: Theresa <twellington@chromium.org>

Gerrit-CC: Chromium LUCI CQ <chromium-scoped@luci-project-accounts.iam.gserviceaccount.com>

Gerrit-CC: Tricium <tricium-prod@appspot.gserviceaccount.com>

Gerrit-CC: chromium-reviews@chromium.org

Gerrit-Attention: Ramin Halavati <rhalavati@chromium.org>

Gerrit-Attention: Theresa <twellington@chromium.org>

Gerrit-Comment-Date: Fri, 18 Jun 2021 15:23:01 +0000

Gerrit-HasComments: Yes

Gerrit-Has-Labels: Yes

Comment-In-Reply-To: Ramin Halavati <rhalavati@chromium.org>

Comment-In-Reply-To: Theresa <twellington@chromium.org>

Gerrit-MessageType: comment

EXHIBIT 7
Redacted in its
Entirety

EXHIBIT 8
Redacted in its
Entirety

EXHIBIT 9
Redacted in its
Entirety

EXHIBIT 10
Redacted in its
Entirety

EXHIBIT 11
Redacted in its
Entirety

EXHIBIT 12
Redacted in its
Entirety

EXHIBIT 13
Redacted in its
Entirety

EXHIBIT 14

Google Chrome Privacy Whitepaper

Last modified: September 30, 2020 (Current as of Chrome 84.0.4147.135)

Omnibox | Network predictions | Search locale | New Tab page | Touch to Search | Search with Google Lens | Safe Browsing protection | Safety Check | Unwanted software protection | Offline Indicator | Google update | Network time | Counting install | Measuring promotions | Usage stats | Google Surveys | Spelling suggestions | Translate | Image Descriptions | Signing In | Autofill | Payments | Geolocation | Speech to text | Google Assistant on Chrome OS devices | Google Assistant on Android devices | Cloud Print | SSL certificate error reporting | Installed apps | Push Messaging | Chrome custom tabs | Continue where you left off | Chrome variations | Do Not Track | Plugins | Media licenses | MediaDrm provisioning | Cloud policy | Lite Mode (Chrome mobile) | Kid’s Google Account | Incognito and Guest mode | Handoff support | Security key | Physical web | Bluetooth | Data sent by Android | Integration with Digital Wellbeing |

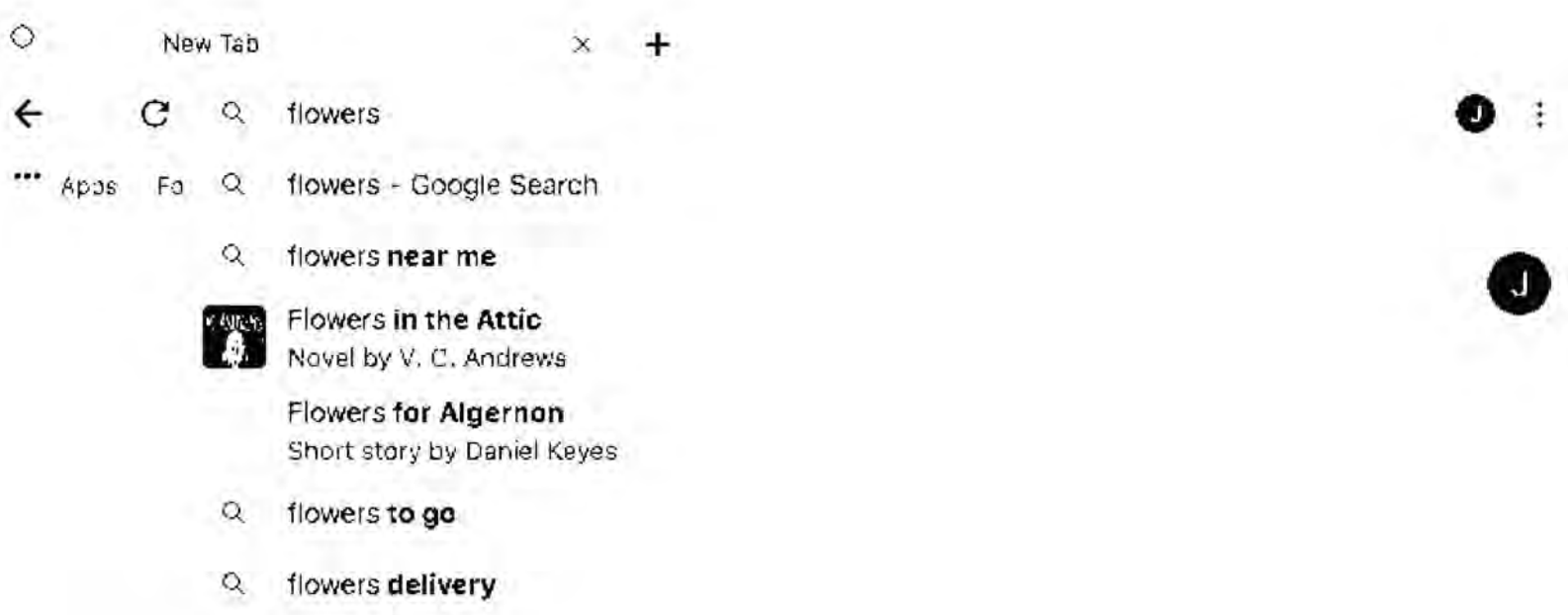
This document describes the features in Chrome that communicate with Google, as well as with third-party services (for example, if you've changed your default search engine). This document also describes the controls available to you regarding how your data is used by Chrome. Here we’re focusing on the desktop version of Chrome; we touch only tangentially on Chrome OS and Chrome for Mobile. This document does not cover features that are still under development, such as features in the beta, dev and canary channel and active field trials, or Android apps on Chrome OS if Play Apps are enabled.

If you have a question about Google Chrome and Privacy that this document doesn’t answer, please feel free to ask it in the [Community Forum](#). If you want to report a privacy issue, you can file it in [our public bug tracker](#). For issues that include confidential information, please use [this link](#). We’d be happy to hear from you.

Omnibox

Google Chrome uses a combined [web address and search bar](#) (we call it the “omnibox”) at the top of the browser window.

As you use the omnibox, your [default search engine](#) can suggest addresses and search queries that may be of interest to you. These suggestions make navigation and searching faster and easier, and are turned on by default. They can be turned off by unchecking "Autocomplete searches and URLs" in the “Sync and Google services” section of Chrome's settings.



When not in Incognito mode, in order to provide these suggestions, Chrome sends the text you've typed into the omnibox, along with a general categorization (e.g., "URL", "search query", or "unknown"), to your default search engine. Chrome will also send a signal to your default search engine when you focus in the omnibox, telling it to get ready to provide suggestions. That signal includes the URL of the currently displayed search engine results page. Your IP address and certain cookies are also sent to your default search engine with all requests, in order to return the results that are most relevant to you.

To provide suggestions and search results faster, Chrome may preconnect to your default search engine in the background. Chrome will not preconnect if you have either turned off “Preload pages for faster browsing and searching” in the “Cookies” part of “Privacy and security” section or "Autocomplete searches and URLs" in the “Sync and Google services” section of Chrome's settings. When Chrome preconnects, it resolves the search engine’s IP address and connects it to the search engine, exposing your IP address.

When in Incognito mode, in order to provide these suggestions, Chrome relies on an on-device model that does not communicate with your default search engine until you select a suggestion.

If Chrome determines that your typing may contain sensitive information, such as authentication credentials, local file names, or URL data that is normally

If Google is your default search engine, when you select one of the omnibox suggestions, Chrome sends your original search query, the suggestion you selected, and the position of the suggestion back to Google. This information helps improve the quality of the suggestion feature, and it's logged and anonymized in the same manner as Google web searches. Logs of these suggestion requests are retained for two weeks, after which 2% of the log data is randomly selected, anonymized, and retained in order to improve the suggestion feature.

If you've chosen to sync your Chrome history, and if Google is your default search engine, the URL of the page you're viewing is sent to Google in order to provide better, contextually relevant suggestions. URLs are sent only for HTTP pages and HTTPS pages, not other schemes such as file: and ftp:. Additionally, Chrome may present website and search query suggestions as soon as you place the cursor in the omnibox, before you start typing. Chrome is in the process of transitioning to a new service to provide these on-focus suggestions. For most users on desktop versions of Chrome, the request and complete set of suggestions are retained on Google servers in order to further improve and personalize the feature. When the URL that triggered the set of suggestions is deleted from your history, the set of suggestions will stop influencing suggestions personalized to you, and will be deleted; otherwise they are retained in your Google account for a year. For a small portion of users on desktop versions of Chrome, and users on mobile versions of Chrome, the logging described in the previous paragraphs apply except that URLs are never included in the 2% sampling of log data.

On Android, your location will also be sent to Google via an X-Geo HTTP request header if Google is your default search engine, the Chrome app has the permission to use your geolocation, and you haven't blocked geolocation for www.google.com (or country-specific origins such as www.google.de). Additionally, if your device has network location enabled (High Accuracy or Battery Saving Device Location mode in Android settings), the X-Geo header may also include visible network IDs (WiFi and Cell), used to geocode the request server-side. The X-Geo header will never be sent in Incognito mode. HTTPS will be required to include this header in the request. You can learn more about how to control the Android OS location sharing with apps on [this article](#) for Nexus, or find your device [here](#) if you do not use a Nexus. How to control location sharing with a site within Chrome is written in [this article](#). See the [Geolocation](#) section of this whitepaper for more information on default geolocation permissions.

Additionally, if Google is your default search engine and you have enabled sync, omnibox may also show suggestions for your Google Drive files. You can turn this functionality off by disabling the "Drive suggestions" option in the "Sync and Google services" section of Chrome's settings.

If you use a non-Google search provider as your default search engine, queries are sent and logged under that provider's privacy policy.

Additionally, when you use the omnibox to search for a single word, Chrome may send this word to your DNS server to see whether it corresponds to a host on your network, and may try to connect to the corresponding host. This gives you the option to navigate to that host instead of searching. For example, if your router goes by the hostname "router", and you type "router" in the omnibox, you're given the option to navigate to <https://router/>, as well as to search for the word "router" with your default search provider. This feature is not controlled by the "Use a prediction service to help complete searches and URLs..." option because it does not involve sending data to your default search engine.

Network predictions

Chrome uses a service to predict which resources and pages are likely to be needed next in order to load pages more quickly. The prediction service uses navigation history, local heuristics, and data learned from Google's search crawlers. Retrieving the data from Google's crawlers requires sending the URL of the current page to Google, and so it is only used if you've opted into "Make Searches and Browsing Better (Sends URLs of the pages you visit to Google)" and/or enabled Lite Mode. The prediction service may initiate actions such as DNS prefetching, TCP and TLS preconnection, and prefetching of web pages. To [turn off](#) network predictions, uncheck "Preload pages for faster browsing and searching" in the "Privacy and security > Cookies" section of Chrome's settings on desktop, in the "Privacy" section of Chrome's settings on Android, and in the "Bandwidth" section of Chrome's settings on iOS.

To improve load times, the browser can be asked to prefetch links that you might click next. Chrome supports five types of prefetching:

- Chrome prefetching - can be initiated by Chrome itself whenever it detects a search query typed in the omnibox, a likely beginning of a URL you type often in the omnibox, or when you have Lite mode enabled and are visiting Google Search.
- Webpage prefetching - requested by one web page to prefetch another
- AMP prefetching - can be requested only by the Google Search App on Android to prefetch several accelerated mobile pages (AMP) articles and display them later in a Chrome Custom Tab
- CustomTabs prefetching - any Android app can request to prefetch several URLs to speed up displaying them later in a Chrome Custom Tab
- Privacy-preserving search result link prefetching - for Lite mode users

Controlling the feature. All prefetching types except webpage prefetching are controlled by Chrome's prediction service setting. Webpage prefetching is allowed regardless of whether Chrome's network prediction service feature is enabled.

Handling of cookies. Except for the Lite mode-only prefetching case, the prefetched site is allowed to set and read its own cookies even if you don't end up visiting the prefetched page, and prefetching is disabled if you have chosen to block third-party cookies. In the Lite mode-only case, prefetching is disabled if you have a cookie for the site, and the site can only set a cookie once you click on the link that was prefetched (see the [Lite mode](#) section for more details).

Javascript execution. For AMP prefetching the page is fully rendered and Javascript is also executed. For the remaining types of prefetching Javascript is not executed.

If Google is set as your default search engine, Chrome will try to determine the most appropriate locale for Google search queries conducted from the omnibox in order to give you relevant search results based on your location. For example, if you were in Germany, your omnibox searches may go through google.de instead of google.com.

In order to do this, Chrome will send a request to google.com each time you start the browser. If you already have any cookies from the google.com domain, this request will also include these cookies, and is logged as any normal HTTPS request to google.com would be (see the description of “server logs” in the privacy key terms for details). If you do not have any cookies from google.com, this request will not create any.

New Tab page

The Chrome New Tab page may display suggestions for websites that you might want to visit.

In order to help you get started, Chrome may suggest content that is popular in your country or region. Chrome uses your IP address to identify your country or region.

Chrome tries to make personalized suggestions that are useful to you. For this, Chrome uses the sites you have visited from your local browsing history. On Android, the most popular languages of the sites you visited may also be sent to Google to provide suggestions in languages you prefer to read, and the device display DPI may be sent to format content for your device. To save data, Chrome may additionally send a hash of the content that Google provided to you the last time, so that you only download content when there is something new.

If you are signed into Chrome, suggestions are *also* based on data stored in your Google account activity. You can control the collection of data in your Google account at Activity controls and manage your account activity at My Activity. For example, if you sync your browsing history and have enabled its use in your Web & App activity, Google may suggest sites that relate to sites you have visited in the past. Chrome measures the quality of suggestions by sending Google information about the sets of suggestions that were displayed, and those that were selected.

On the desktop version of Chrome, you may also manually add shortcuts to websites that you regularly visit, or edit Chrome’s existing website suggestions. After you add, edit, or delete a shortcut to a website, the Chrome New Tab page will not suggest any new websites to you.

Suggestions generated from your browsing history will be removed once you clear your browsing history. However, if you customized your suggestions, they will not be removed.

For Chrome on Android, in certain countries, Chrome may download the content of the New Tab page suggestions from Google, for use while offline. Chrome sends to Google a cookieless request with the URL for each suggestion, along with Chrome’s user agent string, in order to render the content. You can remove downloaded content by clearing Chrome’s cache data, or by opening the Downloads menu and selecting individual pages to delete. You can disable this feature by disabling “Download articles for you on Wi-Fi” in Chrome’s Downloads settings.

For Chrome on Android, if you’re signed in to Chrome, your preferences for the suggested articles can be modified or removed using the “Manage Interests” option from the three dots menu. Your preferences will be sent to Google so that better suggestions are provided to you in the future. For example, if you indicate that you’re not interested in a particular topic or publisher, suggestions about that topic or publisher will not be shown in the future. Likewise, you can indicate that you’re not interested in a specific article via the “Hide story” option in the article’s three dots menu. Suggestions are also personalized based on your interactions with the suggested articles (for example, tapping on or ignoring an article). You can manage this interaction data, which is stored in the Discover section of your Google account, at My Activity.

For desktop and Android versions of Chrome, when you open a new tab, Chrome loads a New Tab page customized by your default search engine (e.g., google.com) if it’s available. This page is preloaded in the background and refreshed periodically so that it opens quickly. Your IP address and cookies, as well as your current browser theme, are sent to your search engine with each refresh request so that the New Tab page can be correctly displayed. See the Embedded Search API for more details. Your search engine may also record your interactions with the New Tab page.

The New Tab page content may be designed by your default search provider. Suggested websites are embedded by Chrome into the New Tab page in a way that does not expose them to your default search provider.

If your default search provider is Google, the New Tab page also contains a web address and search bar that behaves like the omnibox.

This information about the New Tab page may not apply if you've installed an extension that overrides the New Tab page.

Touch to Search

When you select a word, the word, the surrounding text, the languages you speak (from Chrome's Languages settings), and the home country of your device's SIM card are sent to Google to identify recommended search terms (for example, selecting "whale" on a site about the blue whale would lead to the selection expanding to show "blue whale"). The selected word is logged in accordance with standard Google logging policies, and the surrounding text and home country are logged only when the page is already in Google's search index. If you have turned on "Make searches and browsing better", the URL of the page is also sent and logged, and is used to improve your query suggestions.

When Google returns a search suggestion, a card appears that may present an action or additional information related to the search. Opening this card is considered a regular search and navigation on Google, so standard logging policies apply.

Adjusting a selection causes a search for the exact selection. For example, if the user selects "climate" and the selection is automatically expanded to "climate change", the user can adjust the selection back to just "climate" and opening the panel would show full search results for "climate" rather than "climate change". Saying "Ok Google" after selecting a word provides the word and its surrounding text as context for the Google Assistant.

Touch to Search is enabled in a limited mode by default: potentially privacy-sensitive data, such as the URL and surrounding text, is not sent for HTTPS pages. Touch to Search can be fully enabled and disabled in the card or in the Chrome privacy settings.

Search with Google Lens

On Android Chrome, if Google is selected as the default search engine and a recent version of the Google app is installed on your device, touching & holding on an image will present you with an option to initiate a search with Google Lens.

A tap on that menu item will redirect you to the Lens experience in the Google App and the image bytes of the selected image will be sent to the Google Lens app. For non-incognito users, the name of the currently signed-in account (if applicable), image tag attributes, and Chrome experiments may also be sent to the Google App. This information is used to improve the user experience within the Lens app.

Triggering a Lens search is considered a regular search and navigation on Google, so standard logging policies apply.

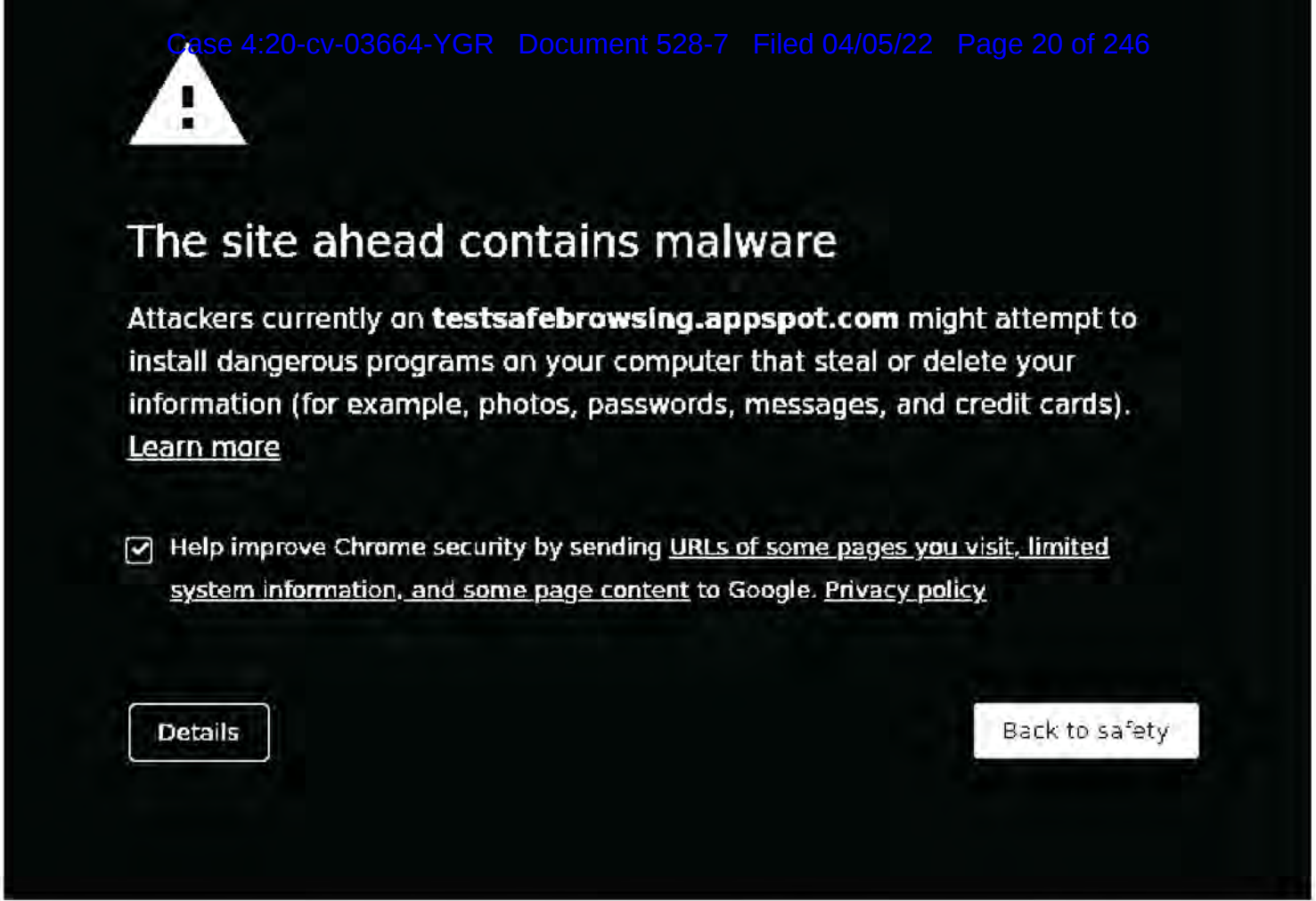
Safe Browsing protection

Google Chrome includes an optional feature called "Safe Browsing" to help protect you against phishing, social engineering, malware, unwanted software, malicious ads, intrusive ads, and abusive websites or extensions. You can find more information at safebrowsing.google.com about how Safe Browsing protects you in Chrome and other Google products. Safe Browsing is designed specifically to protect your privacy and is also used by other popular browsers.

You can find settings for Safe Browsing in the "Privacy and security > Security" section of Chrome's settings. When Safe Browsing is enabled in the "Standard protection" mode (pictured below), Chrome contacts Google's servers periodically to download the most recent Safe Browsing list of unsafe sites including sites associated with phishing, social engineering, malware, unwanted software, malicious ads, intrusive ads, and abusive websites or Chrome extensions. The most recent copy of this list is stored locally on your system. Chrome checks the URL of each site you visit or file you download against this local list. If you navigate to a URL that appears on the list, Chrome sends a partial URL fingerprint (the first 32 bits of a SHA-256 hash of the URL) to Google for verification that the URL is indeed dangerous. Chrome also sends a partial URL fingerprint when a site requests a potentially dangerous permission, so that Google can protect you if the site is malicious. Google cannot determine the actual URL from this information.

In addition to the URL check described above, Chrome also conducts client-side checks. If a website looks suspicious, Chrome sends a subset of likely phishing and social engineering terms found on the page to Google, in order to determine whether the website should be considered malicious. Chrome can also help protect you from phishing if you type one of your previously saved passwords into an uncommon site. In this case Chrome sends the URL and referrers of the page to Google to see if the page might be trying to steal your password.

If you encounter a website that is on Chrome's Safe Browsing list, you may see a warning like the one shown below.



You can [visit our malware warning test page](#) or [social engineering warning test page](#) to see the above example in action. For more information about the warning pages, see [Manage warnings about unsafe sites](#).

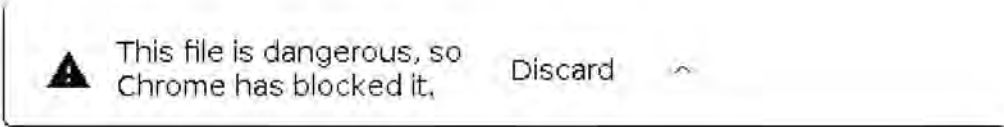
Additionally, if you've opted into "Make Searches and Browsing Better (sends URLs of the pages you visit to Google)", Chrome sends a request to Safe Browsing each time you visit a page that isn't in Chrome's local list of safe sites in order to gather the latest reputation of that website (we call this mechanism "real-time checks"). If you sync your browsing history without a sync passphrase, this request also contains a temporary authentication token tied to your Google account to provide better protections to some users whose account may be under attack. If the website is deemed unsafe by Safe Browsing, you may see a warning like the one shown above. This mechanism is designed to catch unsafe sites that switch domains very quickly or hide from Google's crawlers. Pages loaded in Incognito are not checked using this mechanism.

You can also opt in to reporting additional [data relevant to security](#) to help improve Safe Browsing and security on the Internet. You can opt in by turning on the "Help improve security on the web for everyone" setting in the "Privacy and security > Security" section of Chrome's settings. You can also opt in from the warning page shown above. If you opt in, Chrome will send an incident report to Google every time you receive a warning, visit a suspicious page, and on a very small fraction of sites where Chrome thinks there could be threats, to help Safe Browsing learn about the new threats you may be encountering. Additionally, some downloaded files that are suspicious and show a warning may be sent to Google for investigation each time they are encountered. All reports are sent to Google over an encrypted channel and can include URLs, headers, and snippets of content from the page and they never include data from browsing you do in Incognito mode. If Chrome discovers unwanted or malicious software on your machine, the reports may also include details about malicious files and registry entries. This data is used only to improve Safe Browsing and to improve security on the Internet. For example, Chrome reports some [SSL certificate](#) chains to Google to help improve the accuracy of Chrome's SSL warnings.

Please be aware that if you disable the Safe Browsing feature, Chrome will no longer be able to protect you from websites that try to steal your information or install harmful software. We don't recommend turning it off.

If you are a webmaster, developer, or network admin, you can find more relevant information about Safe Browsing on [this page](#).

Safe Browsing also protects you from abusive extensions and malicious software. When Chrome starts, and on each update of the Safe Browsing list, Chrome scans extensions installed in your browser against the Safe Browsing list. If an extension on the list is found, Chrome will disable the extension, offer you relevant information and may provide an option for you to remove the extension or re-enable it. Chrome also sends the particular extension ID to Safe Browsing. Extensions can also be disabled by Chrome if they're determined to be malicious during an [update](#). If you attempt to download a file on Chrome's Safe Browsing list, you'll see a warning like this one:



To warn you about potentially dangerous files, like the picture shown above, Chrome checks the URL of potentially dangerous file types you download against a list of URLs that have been verified. Potentially dangerous file types include both executables and commonly-abused document types. This list is stored locally on your computer and updated regularly. Chrome does not send information to Google for files you download from URLs in this list, or if the file is signed by a verified publisher. For all other unverified potentially dangerous file downloads, Chrome sends Google the information needed to help determine whether the download is harmful, including some or all of the following: information about the full URL of the site or file download, all related referrers and redirects, code signing certificates, file hashes, and file header information. Chrome may then show a warning like the one pictured above.

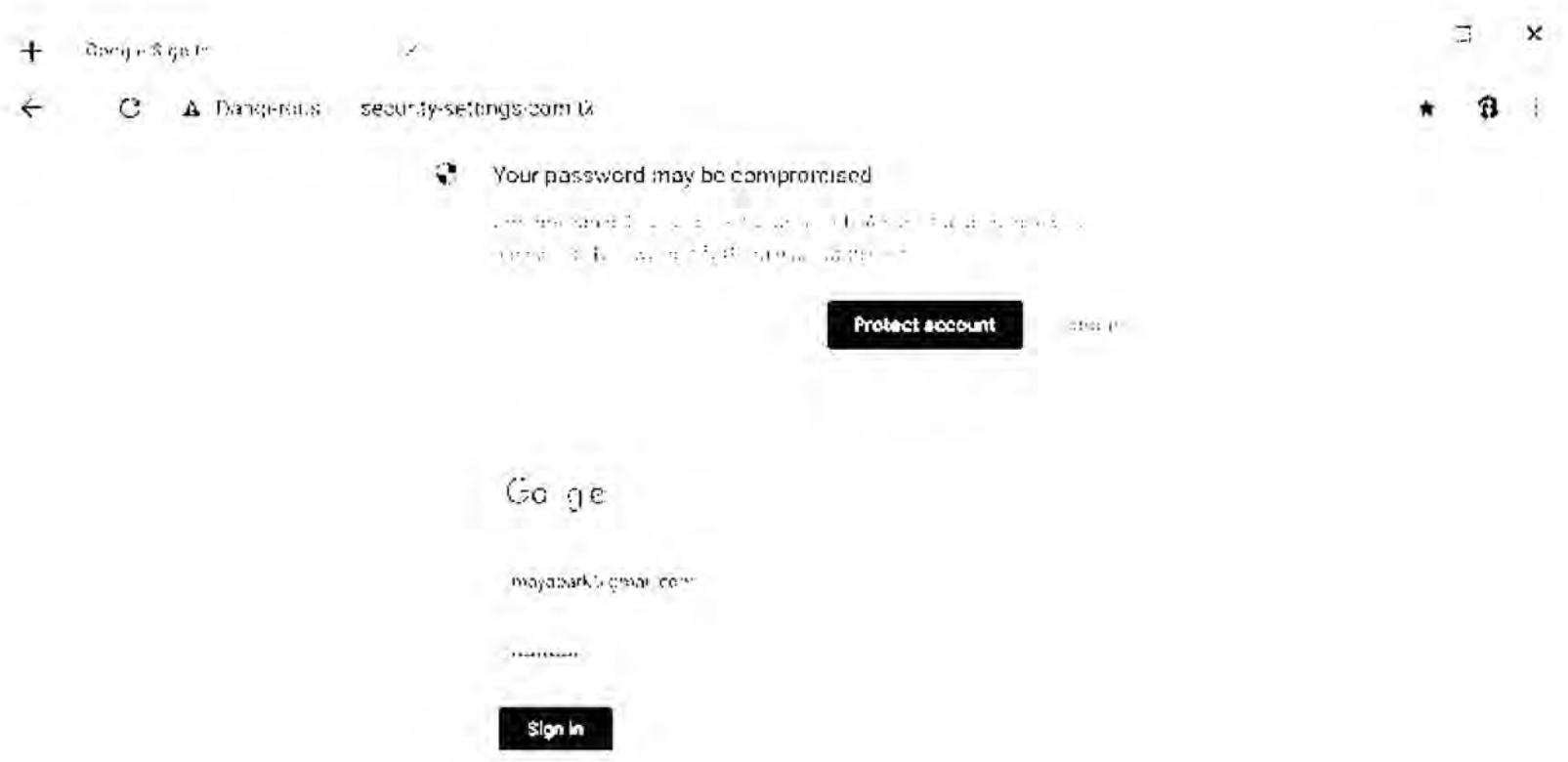
If you are enrolled in [Google's Advanced Protection Program](#), Chrome will show you additional warnings when you download files but where Safe Browsing is unable to ascertain they are safe.

Case 4:20-cv-03664-YGR Document 528-7 Filed 04/05/22 Page 21 of 246

Chrome helps protect you against password phishing by checking with Google when you enter your password on an uncommon page. Chrome keeps a local list of popular websites that Safe Browsing found to be safe. If Chrome detects that you have entered your Google account password or one of your passwords stored in Chrome’s password manager on a website that’s not on the list, it sends a request to Safe Browsing to gather the reputation of that website. The verdict received from Safe Browsing is usually cached on your device for 1 week. For users who have enabled the "Help improve security on the web for everyone" setting, Chrome will ignore the list of popular websites for a small fraction of visits, to test the accuracy of that list.

If the reused password is your Google account password and the verdict for the website is that it is phishing, Chrome will suggest that you change your Google account password to avoid losing access to your account.








If you sync your browsing history without a sync passphrase, or if you accept the “Protect account” option from the dialog shown below, Chrome sends a request to Google to protect your account. This request contains the URL where the phishing attempt happened, and the verdict received from Safe Browsing.



If you've opted into “Help improve security on the web for everyone”, Chrome also sends a request to Safe Browsing each time you start to enter a password on a page that isn’t in Chrome’s local list. In addition, the request Chrome sends to Safe Browsing to determine the reputation of the website on which you reuse your password includes the list of websites for which you saved this password in Chrome’s password manager (but not the password itself).

If Chrome detects that your settings have been tampered with, Chrome reports the URL of the last downloaded potentially dangerous file, and information about the nature of the possible tampering, to the Safe Browsing service.

Chrome asks your permission before using certain web features (APIs) that might have associated risks. Some sites trigger these permission requests in ways users find undesirable or annoying. On these sites Chrome may send the partial URL fingerprint to Google to verify if a less intrusive UI should be used to surface the request.

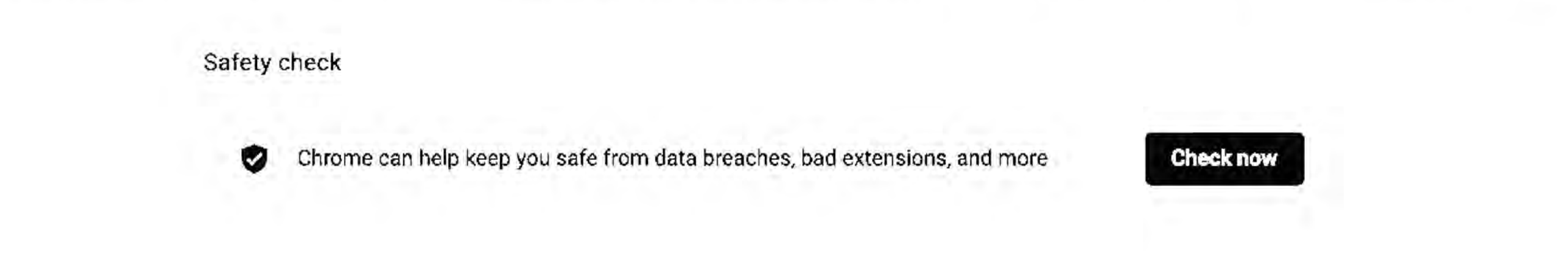
- Enhanced protection**
- ☒ Faster, proactive protection against dangerous websites, downloads, and extensions. Warns you about password breaches. Requires browsing data to be sent to Google.
-  Predicts and warns you about dangerous events before they happen
-  Keeps you safe on Chrome and may be used to improve your security in other Google apps when you are signed in
-  Improves security for you and everyone on the web
-  Warns you if passwords are exposed in a data breach
-  Sends URLs to Safe Browsing to check them. Also sends a small sample of pages, downloads, extension activity, and system information to help discover new threats. Temporarily links this data to your Google Account when you're signed in, to protect you across Google apps.
- Standard protection**
- ☐ Standard protection against websites, downloads, and extensions that are known to be dangerous.
-  Detects and warns you about dangerous events when they happen
-  Checks URLs with a list of unsafe sites stored in Chrome. If a site tries to steal your password, or when you download a harmful file, Chrome may also send URLs, including bits of page content, to Safe Browsing.
- Help improve security on the web for everyone**
- Sends URLs of some pages you visit, limited system information, and some page content to Google, to help discover new threats and protect everyone on the web.
- Warn you if passwords are exposed in a data breach**
- Chrome periodically checks your passwords against lists that have been published online. When doing this, your passwords and usernames are encrypted, so they can't be read by anyone, including Google.

If you've opted into "Enhanced protection" (pictured above), in addition to all the protections described above for "Standard protection" mode, Chrome will use the real-time checks mechanism described above for checking the Safe Browsing reputation of top-level URLs and iframe URLs. If you're signed in to Chrome, the requests for performing real-time checks and the requests for checking potentially dangerous file downloads contain a temporary authentication token tied to your Google account that is used to protect you across Google apps. Enhanced protection also enables reporting additional data relevant to security to help improve Safe Browsing and overall web security, and it enables Chrome's password breach detection. When browsing in incognito or guest mode, these extra checks do not occur, and Enhanced protection mode operates the same way as Standard protection.

For all Safe Browsing requests and reports, Google logs the transferred data in its raw form and retains this data for up to 30 days. Google collects standard log information for Safe Browsing requests, including an IP address and one or more cookies. After at most 30 days, Safe Browsing deletes the raw logs, storing only calculated data in an anonymized form that does not include your IP addresses or cookies. Additionally, Safe Browsing requests won't be associated with your Google Account, except if the request includes the temporary authentication token described above. They are, however, tied to the other Safe Browsing requests made from the same device.

For Chrome on iOS 13 and later, Apple allows for connecting to multiple Safe Browsing services. This means that Chrome may connect to a third-party Safe Browsing service instead of the Google one. Apple determines which Safe Browsing service to connect to based on factors like your device locale.

Safety Check



Unwanted software protection

The Windows version of Chrome is able to detect and remove certain types of software that violate Google's Unwanted Software Policy. If left in your system, this software may perform unwanted actions, such as changing your Chrome settings without your approval. Chrome periodically scans your device to detect potentially unwanted software. In addition, if you have opted in to automatically report details of possible security incidents to Google, Chrome will report information about unwanted software, including relevant file metadata and system settings linked to the unwanted software found on your computer.

If you perform an unwanted software check on your computer from the Settings page, Chrome reports information about unwanted software and your system. System information includes metadata about programs installed or running on your system that could be associated with harmful software, such as: services and processes, scheduled tasks, system registry values commonly used by malicious software, command-line arguments of Chrome shortcuts, Windows proxy settings, and software modules loaded into Chrome or the network stack. You can opt out of sharing this data by deselecting the checkbox next to "Report details to Google" before starting the scan.

If unwanted software is detected, Chrome will offer you an option to clean it up by using the Chrome Cleanup Tool. This will quarantine detected malicious files, delete harmful extensions and registry keys, and reset your settings. The Chrome Cleanup Tool also reports information about unwanted software and your system to Google, and again you can opt out of sharing this data by deselecting the checkbox next to "Report details to Google" before starting the cleanup.

This data is used for the purpose of improving Google's ability to detect unwanted software and offer better protection to Chrome users. It is used in accordance with Google's Privacy Policy and is stored for up to 14 days, after which only aggregated statistics are retained.

Offline Indicator

On Android versions Lollipop and older, when Chrome detects a network change, it sends a cookieless request to http://connectivitycheck.gstatic.com/generate_204 or http://clients4.google.com/generate_204 to determine whether you're offline and display an offline indicator.

Software updates

Desktop versions of Chrome and the Google Chrome Apps Launcher use Google Update to keep you up to date with the latest and most secure versions of software. In order to provide greater transparency and to make the technology available to other applications, the Google Update technology is open source.

Google Update requests include information necessary for the update process, such as the version of Chrome, its release channel, basic hardware information, and update errors that have been encountered. The update requests also send Google information that helps us understand how many people are using Google Chrome and the Chrome Apps Launcher — specifically, whether the software was used in the last day, the number of days since the last time it was used, the total number of days it has been installed, and the number of active profiles. Google Update also periodically sends a non-unique four-letter tag that contains information about how you obtained Google Chrome. This tag is not personally identifiable, does not encode any information about when you obtained Google Chrome, and is the same as everyone who obtained Google Chrome the same way.

Because Chrome OS updates the entire OS stack, Google Update on Chrome OS also sends the current Chrome OS version and hardware model information to Google in order to ensure that the correct software updates and hardware manufacturer customizations such as apps, wallpaper, and help articles are delivered. This information is not personally identifiable, and is common to all users of Chrome OS on the same revision of device.

Unlike the desktop versions of Chrome, the delivery and management of updates for mobile versions of Chrome are managed through the app stores for Android and iOS. Mobile versions of Chrome utilize the servers described above for counting active installations.

Chrome extensions and applications that you've installed are kept up to date with a similar system used for updating desktop versions of Chrome. These update requests include similar information (such as the application ID, when the application was last used, and how long it's been installed). We use these requests to determine the aggregate popularity and usage of applications and extensions. If you are using an extension or application restricted to a certain audience,

authentication tokens are sent with the update requests for these add-ons. For security reasons, Chrome also occasionally sends a cookieless request to the Chrome Web Store, in order to verify that installed extensions and applications that claim to be from the store are genuine.

In order to keep updates as small as possible, Google Chrome is internally split into a variety of components, each of which can be updated independently. Each component is uniquely identified via an ID that is shared among all Google Chrome installations (e.g., "fmeadaodfnidclnjhlkdgjkolmhmfofk"). An update request for a component contains this ID, the hash of the previous download (called a "fingerprint"), and the component's version. Because every installation has the same ID, and downloads of the same component have the same fingerprint, none of this information is personally identifiable.

If you install web apps on an Android device, a Google server is responsible for creating a native Android package that can be verified for authenticity by Chrome. When Chrome is updated or notices that the web app's manifest has changed, Chrome asks the server for a new version of the Android package in a cookieless request. If the information needed to create the native Android package cannot be acquired by the server (e.g., because the information is behind a corporate firewall), Chrome sends it to Google and an Android package is created that is unique to you. It contains a unique and random identifier that is not tied to your identity.

Chrome may also download and run a binary executable (e.g., as part of the software update or to improve Safe Browsing protection). These executables are cryptographically signed and verified before execution. Chrome may download further static resources like dictionaries on demand to reduce the size of the installer.

On Windows and OS X versions of Chrome, the recovery component tries to repair Google Update when it's broken. After the relevant binary is executed, Google Update uploads statistics on the actions that were performed. These statistics contain no personally identifiable information.

Network time

On desktop platforms, Chrome uses network time to verify SSL certificates, which are valid only for a specified time. At random intervals or when Chrome encounters an expired SSL certificate, Chrome may send requests to Google to obtain the time from a trusted source. These requests are more frequent if Chrome believes the system clock is inaccurate. These requests contain no cookies and are not logged on the server.

Counting installations

In order to measure the success rate of Google Chrome downloads and installations of the Windows version of Google Chrome, a randomly-generated token is included with Google Chrome's installer. This token is sent to Google during the installation process to confirm the success of that particular installation. A new token is generated for every install. It is not associated with any personal information, and is deleted once Google Chrome runs and checks for updates the first time.

For Chrome to know how many active installations it has, the mobile version of Chrome sends a ping to Google with a salted hash of a device identifier on an ongoing basis. The desktop version of Chrome does not send any stable identifier to count active installations. Instead an anonymous message to Google with a timestamp of the last ping is used to infer number of active installations.

Measuring effectiveness of a promotion

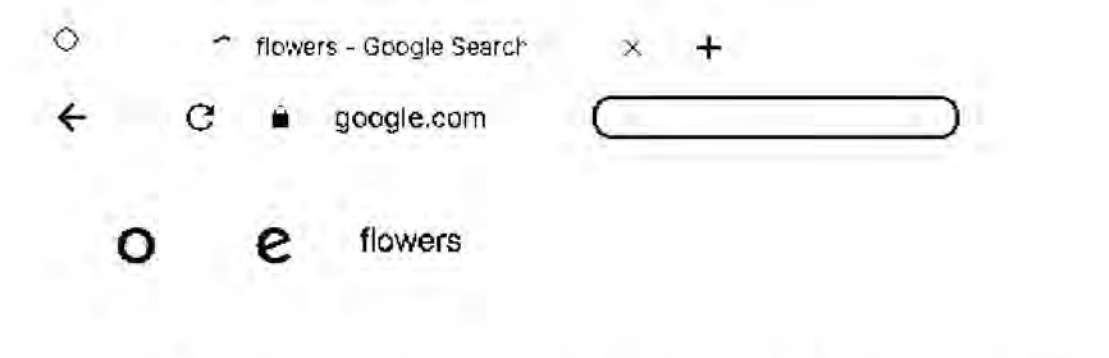
Chrome utilizes two measurements to understand how effective a promotional campaign has been: how many Chrome installations are acquired through a promotional campaign, and how much Chrome usage and traffic to Google is driven by a campaign.

To measure installations or reactivations of Chrome through a campaign, Chrome will send a token or an identifier unique to your device to Google at the first launch of Chrome, as well as the first search using Google. On desktop versions of Chrome, a token unique to your device is generated. The same token will be sent if Chrome is later reinstalled at first launch and at first use of the Omnibox after reinstallation or reactivation. Rather than storing the token on the computer, it is generated when necessary by using built-in system information that is scrambled in an irreversible manner. On iOS, Chrome uses the IDFA for counting installations acquired by a campaign, and it can be reset in iOS settings.

To measure searches and Chrome usage driven by a particular campaign, Chrome inserts a promotional tag, not unique to you or your device, in the searches you perform on Google. This non-unique tag contains information about how Chrome was obtained, the week when Chrome was installed, and the week when the first search was performed. For desktop versions of Chrome, Chrome generates a promotional tag, if the promotional installation token described in the previous paragraph indicates that Chrome has been installed or reactivated by a campaign on a device which has not been associated with any campaign yet. For Chrome on Mobile, a promotional tag is always sent regardless of the source of installations.

The promotional tag is generated using a software library called "RLZ" and looks similar to "1T4ADBR_enUS236US239". The RLZ library was fully open-sourced in June 2010. For more information, please see the In the Open, for RLZ post on the Chromium blog and the article "How To Read An RLZ String". On Android, this promotional tag can also be a readable string like "android-hms-tmobile-us" instead of an RLZ string, and is not unique to either you or your device.

This non-unique promotional tag is included when performing searches via Google (the tag appears as a parameter beginning with "rlz=" when triggered from the Omnibox, or as an "x-rlz-string" HTTP header). We use this information to measure the searches and Chrome usage driven by a particular promotion.

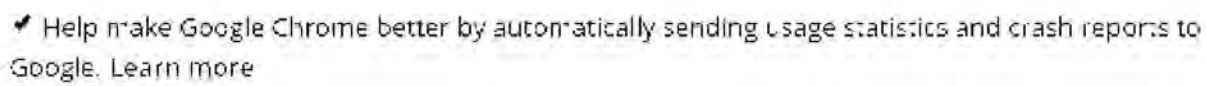


If usage statistics and crash reports are enabled, the RLZ string is sent along with the report. This allows us to improve Chrome based on variations that are limited to specific geographic regions.

For the desktop version of Chrome, you can opt-out of sending this data to Google by uninstalling Chrome, and installing a version downloaded directly from www.google.com/chrome. To opt-out of sending the RLZ string in Chrome OS, press Ctrl + Alt + T to open the crosh shell, type rlz disable followed by the enter key, and then reboot your device.

Usage statistics and crash reports

Chrome has a feature to automatically send usage statistics and crash reports to Google in order to help improve Chrome’s feature set and stability.



Usage statistics contain information such as system information, preferences, user interface feature usage, responsiveness, performance, and memory usage. Crash reports contain system information gathered at the time of the crash, and may contain web page URLs, actions taken by the user before the crash, and/or personal information depending on what was happening at the time of the crash. This feature is enabled by default for Chrome installations of version 54 or later. You can control the feature in the "Sync and Google services" section of Chrome's settings.

When this feature is enabled, Google Chrome stores a randomly generated unique token on your device, which is sent to Google along with your usage statistics and crash reports. The token does not contain any personal information and is used to de-duplicate reports and maintain accuracy in statistics. This token is deleted when the feature is disabled and a new token is regenerated when the feature is enabled again.

By default, the usage statistics do not include any personal information. However, if you're signed in to Chrome and have enabled Chrome sync, Chrome may combine your declared age and gender from your Google account with our statistics to help us build products better suited for your demographics. This demographic data is not included in crash reports.

Along with usage statistics and crash reports, Chrome also reports anonymous, randomized data that is constructed in a manner which is not linked to the unique token, and which ensures that no information can be inferred about any particular user's activity. This data collection mechanism is summarized on the [Google research blog](#), and full technical details have been published in a [technical report](#) and presented at the 2014 ACM Computer and Communications Security conference.

Chrome will also anonymously report to Google if requests to websites operated by Google fail or succeed in order to detect and fix problems quickly.

If you have also turned on “Make searches and browsing better (Sends URLs of pages you visit to Google)” in the “Sync and Google services” section of Chrome’s settings, Chrome usage statistics include information about the web pages you visit and your usage of them. The information will also include the URLs and statistics related to downloaded files. If you sync extensions, these statistics will also include information about the extensions that have been installed from Chrome Web Store. The URLs and statistics are sent along with a unique device identifier that can be reset by turning off “Make searches and browsing better” in the “Sync and Google services” section of Chrome’s settings or by turning off usage statistics and crash reports. The usage statistics are not tied to your Google account. Google only stores usage statistics associated with published extensions, and URLs that are known by Google’s web crawlers. We use this information to improve our products and services, for example, by identifying web pages which load slowly; this gives us insight into how to best improve overall Chrome performance. We also make some statistics available externally, through efforts like the [Chrome User Experience Report](#). Externally published reports are conducted in highly aggregated manner to not reveal individual user's identity.

On iOS, if you are syncing your browsing history without a sync passphrase, Chrome reports usage for certain URLs that other Google apps could open. For example, when you tap on an email address, Chrome presents a dialog that allows you to choose between opening with Google Gmail or other mail apps installed on your device. The usage information also includes which apps were presented to you, which one was selected, and if a Google app was installed. Chrome does not log the actual URL tapped. If you are signed in, this usage is tied to your Google account. If you are signed out, the information is sent to Google with a unique device identifier that can be regenerated by resetting the Google Usage ID found in Chrome settings. The raw reports are deleted within 60 days, after which only the aggregated statistics remain.

language by choosing “Always translate” in the Translate UI. Additionally, you can do so by clicking on a translated search result on the Google Search Results Page.

If you do choose to translate a web page, the text of that page is sent to [Google Translate](#) for translation. Your cookies are not sent along with that request and the request is sent over SSL. This communication with Google's translation service is covered by the [Google privacy policy](#).

If you’ve chosen to sync your Chrome history, statistics about the languages of pages you visit and about your interactions with the translation feature will be sent to Google to improve Chrome’s understanding of the languages you speak and when Chrome should offer to translate text for you.

Image Descriptions for screen reader users

Chrome can provide automatic descriptions for users who are visually impaired by sending the contents of images on pages you visit to Google's servers. This feature is only enabled when Chrome detects that the user has a screen reader running and if the user explicitly enables it in the page context menu. Cookies are not sent along with these requests. Chrome fetches the list of supported languages from Google's servers and then requests descriptions in the most appropriate language given the current web page and the user's language preferences. Requests are not logged.

Sign In to Chrome and sync

You have the option to use the Chrome browser while signed in to your Google Account, with or without [sync](#) enabled.

On desktop versions of Chrome, signing into or out of any Google web service, like google.com, signs you into or out of Chrome. If you are signed in to Chrome, Chrome may offer to save your payment cards and related billing information to your Google Payments account. Chrome may also offer you the option of filling payment cards from your Google Payments account into web forms. If you would like to sign into Google web services, like google.com, without Chrome asking whether you want to save your info to your Google Account, you can [turn off Chrome sign-in](#).

When you’re signed-in and have enabled sync with your Google Account, your personal browsing data information is saved in your Google Account so you may access it when you sign in and sync to Chrome on other computers and devices. Synced data can include bookmarks, saved passwords, open tabs, browsing history, extensions, addresses, phone numbers, payment methods, and more. In advanced sync settings, you can choose which types of data to synchronize with this device. By default, all syncable data types are enabled. You can turn sync on or off in the “You and Google” section of Chrome settings.

If you have turned on sync and signed out of the account you are syncing to, sync will pause sending all syncable data to Google until you sign back in with the same account. Some sync data types (such as bookmarks and passwords) that are saved locally while sync is paused will automatically be synced to your account after you sign back in with the same account.

On mobile versions of Chrome, you can sign into or sign out of Chrome from Chrome settings. Signing into Chrome will also turn on sync. This can be done for any account that has already been added to the mobile device without authenticating again.

On both desktop and mobile, signing into Chrome keeps you signed into Google web services until you sign out of Chrome. On mobile, signing into Chrome will keep you signed in with all Google Accounts that have been added to the device. On desktop, it will keep you signed in with all Google Accounts that you added from a Google web service, unless you have set “Clear cookies and site data when you quit Chrome” in your [cookie settings](#).

On Android and desktop, Chrome signals to Google web services that you are signed into Chrome by attaching an X-Chrome-Connected and/or C-Chrome-ID-Consistency-Request header to any HTTPS requests to Google-owned domains. On iOS, the CHROME_CONNECTED cookie is used instead. This allows those Google web services to update their UI accordingly. If you are using a managed device, your system admin may disable the sign in feature or require that data be deleted when you disconnect your account.

Users can share phone numbers and text between their devices (mobile or desktop) when they are signed-in to Chrome. The transferred data is encrypted during transit and Google cannot read or store the content. To let users select the device to share with, Chrome collects the following information about devices on which a user is signed-in and stores that in the user's Google account: device manufacturer, model number, Chrome version, OS, and device type.

Google uses your personal synchronized data to provide you a consistent browsing experience across your devices, and to customize features in Chrome. You can manage your synchronized history by going to chrome://history in your Chrome browser. If “Include history from Chrome and other apps in your Web & App Activity” is checked on the [Web & App Activity](#) controls page, Google also uses your synchronized browsing data to provide personalized Google products and services to you. You can change your preference any time, and manage individual [activities associated with your Google account](#).

The paragraph above describes the use of your personal browsing history. Google also uses aggregated and anonymized synchronized browsing data to improve other Google products and services. For example, we use this information to improve Google Search by helping to detect mobile friendly pages, pages which have stopped serving content, and downloads of malware.

Case 4:20-cv-03664-YGR Document 528-7 Filed 04/05/22 Page 28 of 248

If you would like to use Google's cloud to store and sync your Chrome data without allowing any personalized and aggregated use by Google as described in the previous paragraphs, you can choose to encrypt all of your synced data with a [sync passphrase](#). If you choose this option, it's important to note that Google won't have access to the sync passphrase you set; we won't be able to help you recover data if you forget the passphrase. Regardless of how you choose to encrypt your data, all data is always sent over secure SSL connections to Google's servers.

Google will store the metadata about the days on which sync was running to improve other Google products and services.

If you're signed into Chrome and are syncing passwords and/or other types of login credentials without a sync passphrase, these credentials are stored in your Google Account. Chrome may help you sign in with credentials you've saved in Android apps on websites that are associated with the respective apps. Likewise, credentials you've saved for websites can be used to help you sign into related Android apps. You can view the credentials you've saved in Chrome and Android by visiting [passwords.google.com](#) in any browser. If you've saved credentials for Android applications, Chrome periodically sends a cookieless request to Google to get an updated list of websites that are associated with those applications. To stop websites and Android apps from automatically signing in using credentials you previously saved, you can turn off Auto Sign-In on [passwords.google.com](#) or in Chrome settings under "Autofill > Passwords". For more details see [this article](#).

To make the history page easier to use, Chrome displays favicons of visited URLs. For Chrome browsing history from your other devices, these favicons are fetched from Google servers via cookieless requests that only contain the given URL and device display DPI. Favicons are not fetched for users with sync passphrase.

On the iOS version of Chrome, if you sync your browsing history without a sync passphrase and your browser's usage statistics and crash reports setting is also enabled, your usage statistics and crash reports will include statistics about the pages you visit. You can read more in the [Usage statistics and crash reports](#) section of this Whitepaper.

All data synchronized through Google's servers is subject to [Google's Privacy Policy](#). To get an overview of the Chrome data stored for your Google Account, go to the [Chrome section of Google Dashboard](#). That page also allows you to stop synchronization completely and delete all sync data from Google's servers.

Autofill and Password Management

Google Chrome has a [form autofill feature](#) that helps you fill out forms on the web more quickly. Autofill is enabled by default, but it can be turned off at any time in Chrome's settings.

If Autofill is enabled and you encounter a web page containing a form, Chrome sends some information about that form to Google. This information includes the basic structure of the form, a hash of the web page's hostname as well as form identifiers (such as field names); randomized representation of the form identifiers, and if you have turned on the "Make searches and browsing better (Sends URLs of pages you visit to Google)" setting, also a randomized representation of the web page's URL. In response, Chrome receives a prediction of each field's data type (for example, "field X is a phone number, and field Y is a country"). This information helps Chrome match up your locally stored Autofill data with the fields of the form.

If Autofill is enabled when you *submit* a form, Chrome sends Google some information about the form along with the types of data you submitted. This information includes a hash of the web page's hostname, as well as form identifiers (such as field names), the basic structure of the form, and the observed data types for the fields (i.e., field X was a phone number, field Y was a country). The values you entered into the form are not sent to Google. This information helps Chrome improve the quality of its form-filling over time.

You can manage your Autofill entries via [Chrome's settings](#), and you can edit or delete saved information at any time. Chrome will never store full credit card information (card number, cardholder name, and expiration date) without explicit confirmation. In order to prevent offering to save cards you have shown disinterest in saving, Chrome stores the last four digits of detected credit cards locally on the device. If you scan your credit card using a phone camera, the recognition is performed locally.

Chrome may help you sign in to websites with credentials you've saved to Chrome's password manager or Google Smart Lock by autofilling sign-in forms, by offering you an account picker, or by automatically signing you in. You can manage and delete your saved credentials in the "Forms and passwords" section of Chrome's settings. If you enable [password management](#), the same kind of data about forms as described above is sent to Google to interpret password forms correctly. To enable Chrome to offer password generation that meets site-specific requirements, Chrome uploads a randomized vote on a specific password characteristic to the server once a user-created password is stored. If stored credentials are used for the first time in a username field which was already filled differently by the website itself, Chrome also transmits a short one-byte hash of the prefilled value. This allows Google to classify if the website uses a static placeholder in the username field which can be safely overwritten without deleting valuable user-specific data. Google cannot reconstruct the value from this hash.

When you sign in to a site, Chrome can give you a [warning](#) if the username/password have been exposed as a result of a data breach on some website or app. The feature is available on all platforms but only to the users signed in with a Google account. On Android the feature is only available if sync is also enabled, due to the way the accounts are managed by the OS. Being signed in to a Google account is a technical requirement that prevents abuse of the API. When you sign in to a website, Chrome will send a hashed copy of your username and password to Google encrypted with a secret key only known to Chrome. [No one, including Google, is able to derive your username or password from this encrypted copy](#). From the response, Chrome can tell if the submitted username and password

appear in the database of leaked credentials. The final resolution is done locally; Google doesn't know whether or not the credential is present in the database. The feature can be disabled in settings under Sync and Google services. On desktop and Android versions of Chrome, this feature is not available if Safe Browsing is turned off.

Using the same secure method described above, you can check all the saved passwords against the public data breaches in the “Passwords” section of Chrome’s settings. Once you’ve run a password check, Chrome will show a list of breached passwords. If a password in this list is outdated, you can manually edit it to store the current version. If you choose to edit, the new username/password pair will be checked automatically but only if the feature described above is not disabled.

Also, if you choose, you can bring your Autofill data with you to all your Chrome-enabled devices by [syncing it](#) as part of your browser settings (see the “Sign In to Chrome” section of this document). If you choose to sync Autofill information, field values are sent as described in “Sign In to Chrome”; otherwise, field values are not sent.

Payments

When you’re signed into Chrome with your Google Account, Chrome may offer to save payment cards and related billing addresses into payment data under the same Google Account, and include cards from your account among the autofill suggestions on payment web forms. If you're not signed in, Chrome offers to save your credit cards locally. If the card is not stored locally, you will be prompted for your CVV code or device authentication, such as Touch ID or Windows Hello, each time you use the card. In some versions of Chrome, it is possible to store a card to Google Payments and locally in Chrome at the same time, in which case Chrome will not ask for a CVV or device authentication confirmation. If you have cards stored in this way, their local copies will persist until you sign out of your Google account, at which point the local copy will be deleted from your device. If you choose not to store the card locally, you will be prompted for your CVV code or device authentication each time you use the card. You can [opt out of using device authentication](#) in the Payment methods section of Chrome settings. If you use a card from Google Payments, Chrome will collect information about your computer and share it with Google Payments to prevent fraudulent use of your card.

To delete credit card information saved in Chrome, follow the “Add and edit credit cards” steps in [the Autofill article](#). When you delete a credit card that's also saved in your Google Payments account, you will be redirected to Google Payments to complete the deletion. After your card has been deleted from your Google Payments account, Chrome will automatically remove that card from your Autofill suggestions.

To save a card locally on the device only, while still being signed in to Chrome with a Google Account, you can add a card from the “Add” button in the “Payment methods” section in Chrome settings. If you would like to sign into Google web services, like google.com, without Chrome asking whether you want to save your info to your Google Account, you can [turn off Chrome sign-in](#). If you have sync turned on, you can disable syncing payment methods and addresses to Google Pay under “Sync” in Chrome settings. You can also turn the Payments Autofill feature off altogether in [settings](#).

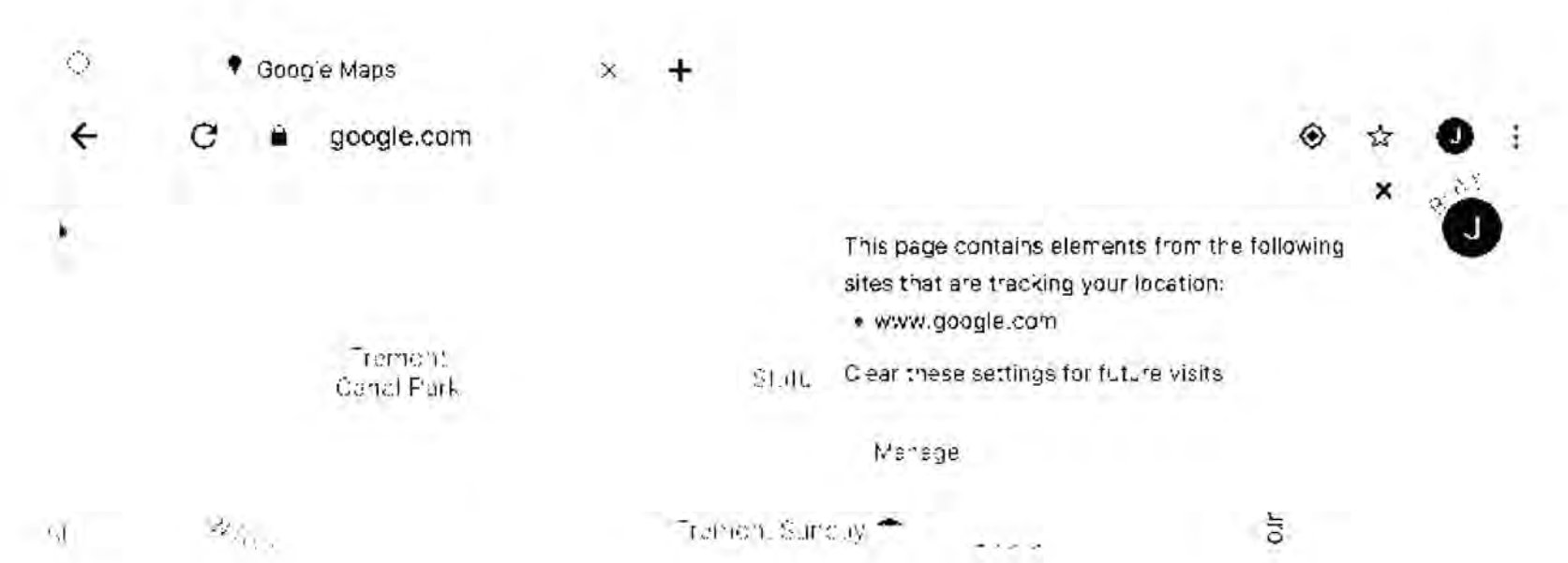
Chrome also supports the [PaymentRequest API](#) by allowing you to pay for purchases with credit cards from Autofill, Google Payments, and other payment apps already installed on your device. Google Payments and other payment apps are only available on Android devices. PaymentRequest allows the merchant to request the following information: full name, shipping address, billing address, phone number, email, credit card number, credit card expiration, CVV, and Google Payments credentials. Information is not shared with the merchant until you agree.

Geolocation

Google Chrome supports the [Geolocation API](#), which provides access to fine-grained user location information with your consent.

By default, Chrome will request your permission when a web page asks for your location information, and does not send any location information to the web page unless you explicitly consent.

Furthermore, whenever you are on a web page which is using your location information, Chrome will display a location icon on the right side of the omnibox. You can click on this icon in order to find out more information or manage location settings.



In Chrome’s settings, by clicking “Site Settings” and scrolling to the “Location” section, you can choose to allow all sites to receive your location information, have Chrome ask you every time (the default), or block all sites from receiving your location information. You can also configure exceptions for specific web sites.

In the Android version of Chrome, your default search engine automatically receives your location when you conduct a search. On the iOS version of Chrome, by default your location is sent to Google if you conduct a search from the omnibox. Read more about how your default search engine handles geolocation and how to manage your settings in the [Omnibox](#) section of the whitepaper.

If you do choose to share your location with a web site, Chrome will send local network information to Google (also used by other browsers such as Mozilla Firefox) in order to estimate your location. This local network information can include data about nearby Wi-Fi access points or cellular signal sites/towers (even if you’re not using them), and your computer’s IP address. The requests are logged, and aggregated and anonymized before being used to operate, support, and improve the overall quality of Google Chrome and Google Location Services.

For further reading on the privacy and user interface implications of the Geolocation API (as well as other HTML5 APIs), see [“Practical Privacy Concerns in a Real World Browser”](#) written by two Google Chrome team members.

Speech to text

Chrome supports the [Web Speech API](#), a mechanism for converting speech to text on a web page. It uses Google's servers to perform the conversion. Using the feature sends an audio recording to Google (audio data is not sent directly to the page itself), along with the domain of the website using the API, your default browser language and the language settings of the website. Cookies are not sent along with these requests.

Google Assistant on Chrome OS devices

The Google Assistant is integrated into some models of Chrome OS devices. If you opt in to the feature, Chrome OS listens for you to say "Ok Google" and sends the audio of the next thing you say, plus a few seconds before, to Google. Detection of the phrase "Ok Google" is performed locally on your computer, and the audio is only sent to Google after it detects "Ok Google". You can enable or disable this feature in Google Assistant Settings.

Enabling this feature in Chrome Settings will cause Chrome to listen whenever the screen is unlocked. On Chrome OS devices with a local audio processor, the device also listens when the device is asleep. On these devices, The Google Assistant feature only works if [Voice & Audio Activity](#) is enabled for your Google account. Chrome will prompt you to enable [Voice & Audio Activity](#) for the associated Google account if it is disabled.

Once the audio has been converted to text, a search with that text is submitted to Google. If you have used the “Ok Google” search before on a device but turned off Voice & Audio Activity later, your device is still capable of processing your voice and sending the audio to Google but the voice is deleted shortly thereafter.

You can determine your Chrome OS device’s behavior by examining the text in the "Search and Assistant" section of settings.

Google Assistant on Android devices

You can quickly complete tasks on the web using the Google Assistant in Chrome on certain Android devices . If you opt-in to this feature, you can speak to the Google Assistant and ask it to search websites. It also can fill out forms on your behalf, or speed up the checkout experience.

For example, if you issue a command to the Google Assistant e.g. “search Wikipedia for Henry VIII”, the Google Assistant in Chrome will respond by opening Chrome to Wikipedia, sending the query as a text string to Google Assistant in Chrome, and searching for “Henry VIII” on the Wikipedia page.

As another example, if you ask the Google Assistant to help you purchase tickets for an upcoming movie, then the address of the website you are viewing, your credit card information, and your email address will be shared with Google to complete the transaction and make it possible for you to receive the purchase receipt and movie ticket.

If you opt-in to this feature, the Google Assistant in Chrome will send data to Google in order to complete the command you issued. When the command is issued, the Google Assistant in Chrome shares back to Google the website’s URL to validate that the webpage is allowed to be automated by Google Assistant in Chrome and to receive the instructions on how to complete the task (e.g. on how to fill out a form).

At the time the command you issued is executed, additional information can be shared. Depending on the command you issued, the information shared with Google can include the address of the website you are viewing, your email address, your name, your delivery and billing address, your credit card information, and possibly the username you use to log into the website. This information is not stored by Google — rather, this information is passed on to the third party website to complete the command you issued to the Google Assistant. Additionally, information about your system is collected in order to improve the product and to debug issues.

To personalize future actions Google Assistant in Chrome will save configuration information about the command you issued to improve your future experiences (for example: seat selections, number and types of movie tickets, etc.). This information is saved to your [Google Account](#).

Some Google Assistant features are not available on Incognito tabs. You can turn off the ability to use the Google Assistant in Chrome on your Android device by toggling the “Google Assistant for Chrome” option in Chrome’s settings.

Google Cloud Print

The [Google Cloud Print](#) feature allows you to print documents from your browser over the Internet. You do not need a direct connection between the machine that executes Chrome and your printer.

If you choose to print a web page via Cloud Print, Chrome will generate a PDF of this website and upload it over an encrypted network connection to Google’s servers. If you choose to print other kinds of documents, they may be uploaded as raw documents to Google’s servers.

A print job will be downloaded by either a Chrome browser (“Connector”) or a Cloud Print capable printer that you selected when printing the website. In some cases the print job must be submitted to a third-party service to print (HP’s ePrint, for example).

The print job is deleted from Google’s servers when any of three criteria is met:

- You delete the print job
- The job has been printed and marked as printed by the printer/connector
- The job has been queued on Google’s servers for 30 days

You can manage your printers and print jobs on the [Google Cloud Print website](#).

SSL certificate reporting

Chrome stores locally a list of expected SSL certificate information for a variety of high-value websites, in an effort to [prevent man-in-the-middle attacks](#). For Google websites and other websites that choose to opt in, Chrome will report a possible attack or misconfiguration. If the certificate provided by the web server doesn’t match the expected signature, Chrome reports information about the SSL certificate chain to Google or to a report collection endpoint of the website's choosing. Chrome sends these reports only for certificate chains that use a [public root of trust](#).

You can enable this feature by opting in to report data relevant to security, as described in the [Safe Browsing section](#). While you are opted in, two kinds of reports may be sent to Google’s security team. Each time you see an SSL error page, a report will be sent containing the SSL certificate chain, the server’s hostname, the local time, and relevant details about the validation error and SSL error page type. Additionally, each time a mismatch between different certificate verifiers is detected, a report will be sent containing the certificate chain and the verification result.

Because Chrome sends these reports for all certificate chains, even those that chain to a private root of trust, these chains can contain personally identifiable information. You can opt out anytime by unchecking the box “Help Improve Chrome security” in “Privacy and security > Security”.

The SSL certificate reporting feature is not available on Chrome iOS.

Installed Applications and Extensions

Users can install external apps and extensions for the desktop versions of Chrome to add features to or customize their Chrome browsers. Installing an application or extension from the Chrome Web Store directly or via an [inline installation](#) flow on a third-party site involves a request to the Chrome Web Store for details about the application. This request includes cookies, and if you’re logged into Google when you install an application, that installation is recorded as part of your Google account. The store uses this information to recommend applications to you in the future, and in aggregate to evaluate application popularity and usage. As noted above, applications and extensions are updated via Google Update.

As they're more deeply integrated into Chrome, applications and extensions that you choose to install can request access to additional capabilities, enabling functionality that doesn't make sense on the web at large: background notifications or raw socket access, for instance. These additional permissions may change the way your data is collected and shared, as extensions and applications might have access to data regarding the websites you visit, and might be capable of monitoring or modifying your interactions with the web. When installing an application or extension, Chrome may first warn you about [certain capabilities](#). Please do take the time to read and evaluate this warning before proceeding with the installation. Note also that interactions with and data collected by these third-party applications and extensions are governed by their own privacy policies, not Google's privacy policy.

Push messaging

Case 4:20-cv-03664-YGR Document 528-7 Filed 04/05/22 Page 32 of 246

Your device may receive push messages from the backend servers of apps and extensions installed in Chrome, websites that you grant the “notification” permission to, and your default search engine. Disabling push messages from your default search engine is done in the same way as disabling push messages from any site, by visiting the “Notifications” section of “Site settings”.

Push message data is sent over a secure channel from the developer through Google’s infrastructure to Chrome on your device, which can wake up apps, extensions, and websites (including your default search engine) to deliver the message. The developer may end-to-end encrypt the message data, or may send it in a form such that Google servers process it as plain text. Google servers retain up to 4 weeks’ worth of messages to ensure delivery to users even if their devices are offline at the time of the initial pushing.

If the notification permission is set to “granted” for any website (including the default search engine), or you have an app or extension installed that uses push messaging, then Chrome provides the app’s, extension’s, or website’s server with one or more registration tokens that can be used to send messages to the entity (app, extension, or website). Websites you visit in Incognito mode are not allowed to send you push messages and therefore cannot get a registration token.

When you uninstall an app or extension, revoke the notification permission for a website, or clear cookies for a permitted website, its registration token is revoked and will not be reused, even if the same app or extension is re-installed or the same website is re-visited. Registration tokens used by Chrome components such as Sync are revoked once they are no longer in use (for example, when the user disables Sync). When a registration token is revoked, the associated entity on your device stops receiving messages sent from its developer’s server.

The registration tokens that are passed to entities contain an encrypted device ID, which is used for routing the messages. Google can decrypt the device ID, but other entities cannot, and the encryption is designed so that two registration tokens for the same device ID cannot be correlated. On desktop versions of Chrome, the device ID is reset when the Chrome profile is removed, or when neither Chrome Sync nor any of the entities requires it for push messaging. On Android, the lifetime of the device ID is governed by the operating system and is independent of Chrome. Any messages routed to registration tokens containing a revoked device ID will not be delivered.

Chrome custom tabs

On Android devices, an app developer may use a Custom Tab to show web content when you click on a URL from their app. A Custom Tab may look different from a regular Chrome tab, for example it may have app-specified visual style, and the absence of an editable URL bar. Despite the different visual style a Custom Tab may have, the data sent and received in the Custom Tab, such as cookies, saved passwords and browsing history function the same way they do in a normal Chrome tab. The Custom Tab is an app-customized view using the same underlying user profile.

With Chrome Custom Tabs, an Android app developer may also specify custom actions in the Chrome toolbar and overflow menu that are relevant to their app, for example,"share", “save page”, “copy URL”. If you tap on such a button, the address of the current website is shared with the application.

An application can request Chrome to pre-render a given URL in the background. This allows Chrome to show you a pre-loaded site instantly when you open it from the app. At the same time it allows an application to set cookies in your browser in the background. To disable pre-rendering, you can uncheck "Preload pages for faster browsing and searching" in the “Privacy and security > Cookies” section of Chrome’s settings.

Trusted Web Activities are a form of Chrome Custom Tab where the top bar is not present, allowing web browsing with no browser UI but with access to the cookie jar. They can only be used to view web content on an origin that the client app can prove that it owns using Digital Asset Links. If the user navigates off this origin the the top bar reappears.

When the client app is uninstalled or has its data cleared through Android Settings, Chrome will allow the user to clear data for the linked origin.

Continue where you left off

If you have selected the option to “Continue where you left off” in settings on desktop versions of Chrome, when you open Chrome, it attempts to bring you right back to the way things were when the browser was closed. Chrome reloads the tabs you had open and persists session information to get you up and running as quickly as possible. This feature effectively extends a browsing session across restarts. In this mode, session cookies are no longer deleted when the browser closes; instead, they remain available on restart to keep you logged into your favorite sites.

On desktop versions of Chrome, this feature can be enabled or disabled in Chrome settings. On Chrome OS, it is enabled by default.

On OS X, when you restart your device, a checkbox in the OS confirmation dialog asks you whether you want to re-open applications and windows after restart. If you check this box, Chrome restores tabs and windows, as well as the session cookies, even if you have disabled "Continue where you left off" on Chrome.

On mobile versions of Chrome, this feature is always enabled without a setting.

Chrome is constantly evolving to better meet the needs of users and the web. To ensure new features are providing the best experience and working correctly, they may be enabled for a subset of users before they are fully launched. For example, if we improve how page loading works in Chrome, we may try it out for 1% of users to ensure that it doesn't crash or run slower before launching to everyone. This is done through a system called "Chrome Variations" - also known as "field trials".

A given Chrome installation may be participating in a number of different variations (for different features) at the same time. These fall into two categories:

1. Low entropy variations, which are randomized based on a number from 0 to 7999 (13 bits) that's randomly generated by each Chrome installation on the first run.
2. High entropy variations, which are randomized using the usage statistics token for Chrome installations that have usage statistics reporting enabled.

Other factors may additionally inform the variations assigned to a Chrome installation, such as country (determined by your IP address), operating system, Chrome version and other parameters.

Usage statistics and crash reports are tagged with all variations a client participates in, including both low entropy and high entropy variations. These reports, which also contain a pseudonymous client identifier, can be disabled in Chrome settings.

Additionally, a subset of low entropy variations are included in network requests sent to Google. The combined state of these variations is non-identifying, since it is based on a 13-bit low entropy value (see above). These are transmitted using the "X-Client-Data" HTTP header, which contains a list of active variations. On Android, this header may include a limited set of external server-side experiments, which may affect the Chrome installation. This header is used to evaluate the effect on Google servers - for example, a networking change may affect YouTube video load speed or an Omnibox ranking update may result in more helpful Google Search results.

On Android Chrome, in certain cases these low entropy variations may also be sent to Google apps when cross-app communication occurs to support a Chrome feature; for example, when searching with [Google Lens](#). This information is used to better understand how Chrome experiments affect that Google feature: for example, Chrome memory usage change could affect how long it takes an action in the Google app to complete.

You can reset the variations used by your Chrome installation by starting it with the "--reset-variation-state" command line flag.

Do Not Track

If you enable the "Do Not Track" preference in Chrome's settings, Chrome will send a DNT:1 HTTP header with your outgoing HTTP, HTTPS and SPDY browsing traffic (Chrome cannot, however, guarantee that NPAPI plugins also send the header.) The header will not be sent with system traffic such as the geolocation, metrics or device management services.

The effect of Do Not Track depends on whether a website responds to the request, and how the request is interpreted. For example, some websites may respond to this request by showing you ads that aren't based on other websites you've visited. Many websites will still collect and use your browsing data - for example, to improve security; to provide content, services, ads and recommendations on their websites; and to generate reporting statistics.

Chrome on iOS now uses WKWebView to provide a more stable and faster browser. As a result of this move, the Do Not Track preference is no longer available due to iOS constraints. If Apple makes changes to allow this feature, Chrome will make Do Not Track available again in iOS.

Plugins

Chrome ships with an Adobe Flash Player implementation that is based on the Pepper API. Flash and other Pepper-based plugins may ask you for "Access to your computer". If you grant this permission, the plugin is granted unsandboxed access. This allows content providers to offer you access to DRM protected content like videos or music but may have security and privacy implications, so consider carefully whether you trust a plugin or website with this privilege.

Media licenses

Some websites encrypt media to protect against unauthorized access and copying. When users play media from these sites, they typically log into the site, which authenticates the user, and then digital rights management negotiates a key exchange for the decryption and playback of the media.

For HTML5 sites, this key exchange is done using the Encrypted Media Extensions API. The implementation of that API is tightly coupled with the browser to protect user privacy and security, through Content Decryption Modules (CDM), which are provided by digital rights management solutions such as Google Widevine or Microsoft PlayReady.

When a user asks Chrome to play encrypted HTML5 media (for example, watching a movie on Google Play Movies), Chrome will generate a request for a license to decrypt that media. This license request contains an automatically generated request ID, which is created by the Content Decryption Module, as well as proof that the CDM is legitimate. After generation, the license request is typically sent to a license server managed by either the content website or Google. Neither the license request, the proof, nor the request ID include any personally identifying information. After being sent, the license request is not stored locally on the user's device.

As part of the license request, Chrome also generates a unique session ID which does not contain personally identifying information. This session ID is sent to the license server, and when the server returns a license the session ID is used to decrypt the media. The session ID may be stored locally even after the site has been closed. The license may also be stored locally for offline consumption of protected content. Session ID and licenses may be cleared by the user in Chrome using [Clear Browsing Data](#) with “Cookies and other site data” selected.

When returning a license, the site license server may include a client ID, generated by the site. This client ID is unique to the user and the site, it is not shared between sites. If provided, the client ID is stored locally and included by Chrome in subsequent license requests to that site. The client ID may be cleared by the user in Chrome using [Clear Browsing Data](#) with “Cookies and other site data” selected.

On some platforms, the website may additionally request verification that the device is eligible to play specific types of protected content. On Chrome OS, this is known as [Verified Access](#). In this case, Google creates a certificate using a unique hardware identifier for the device. This hardware ID identifies the device, but does not identify the user. If the user agrees, Google receives the hardware ID and generates a certificate verifying the device for the requested site. The certificate does not include the hardware ID or any other information that could permanently identify the device. Certificates are stored locally similar to other cached browsing data, and may be cleared by the user in Chrome using [Clear Browsing Data](#) with “Cookies and other site data” selected. On Android, this is called [Provisioning](#). See “[MediaDrm Provisioning](#)” for more details.

Some sites use Flash instead of HTML5. If a website you visit chooses to use Adobe Flash Access DRM protection, Chrome for Windows and Chrome OS will give Adobe Flash access to a device identifier. You can deny this access in the settings under Content Settings, Protected content, and reset the ID using [Clear Browsing Data](#) with “Cookies and other site data” selected.

In order to give you access to licensed music, the [Google Play Music app](#) can retrieve a device identifier that is derived from your hard drive partitions or, on a Chrome OS or Linux installation, from a unique file on your disk. This identifier can be reset by reinstalling your operating system.

MediaDrm provisioning

Chrome on Android uses [Android MediaDrm](#) to play protected content. As on ChromeOS, the website may request verification that the device is eligible to do so. This is achieved by MediaDrm provisioning. A provisioning request is sent to Google, which generates a certificate that will be stored on the device and sent to the site whenever you play protected content. The information in the provisioning request and in the certificate vary depending on the Android version. In all cases, the information can be used to identify the device, but never the user.

On Android K and L, the device only needs to be provisioned once and the certificate is shared by all applications running on the device. The request contains a hardware ID, and the certificate contains a stable device ID, both of which could be used to permanently identify the device.

On Android M or later, MediaDrm supports per-origin provisioning. Chrome randomly generates an origin ID for each website to be provisioned. Even though the request still contains a hardware ID, the certificate is different for each website, so that different websites cannot cross-reference the same device.

On Android O or later on some devices, provisioning can be scoped to a single application. The request will contain a hardware ID, but the certificate will be different for each application, in addition to each site, so different applications cannot cross-reference the same device.

Provisioning can be controlled by the “Protected media” permission in the “Site settings” menu. On Android versions K and L, Chrome will always ask you to grant this permission before provisioning starts. On later versions of Android, this permission is granted by default. You can clear the provisioned certificates anytime using the “Cookies and other site data” option in the [Clear browsing data](#) dialog.

Chrome also performs MediaDrm pre-provisioning to support playback of protected content in cases where the provisioning server is not accessible, such as in-flight entertainment. Chrome randomly generates a list of origin IDs and provision them in advance for future use.

On Android versions with per-device provisioning, where provisioning requires a permission, Chrome does not support pre-provisioning. Playback might still work because the device could have already been provisioned by other applications.

On Android versions with per-origin provisioning, Chrome pre-provisions itself once the user attempts to play protected content. As the provisioning for the first playback already involved sending a stable hardware ID to Google, the subsequent pre-provisioning of additional origin IDs introduces no new privacy implications. If provisioning fails and there is no pre-provisioned origin ID, Chrome may ask for permission to further fallback to per-device provisioning.

Cloud policy

When you sign into a Chrome OS device, Chrome on Android, or a desktop Chrome profile with an account associated with a Google Apps domain, or if your desktop browser is enrolled in Chrome Browser Cloud Management, Chrome checks whether the domain has configured enterprise policies. If so, the Chrome OS user session, Chrome profile, or enrolled Chrome Browser is assigned a unique ID, and registered as belonging to that Google Apps domain. Any configured policies are applied. To revoke the registration, remove the Chrome OS user, sign out of Chrome on Android, remove the desktop profile, or remove the enrollment token and device token for Chrome Browser Cloud Management.

Additionally, Chrome OS devices can be enrolled to a Google Apps domain by a domain admin. This will enforce enterprise policies for the entire device, such as providing shared network configurations and restricting access to developer mode. When a Chrome OS device is enrolled to a domain, then a unique device ID is registered to the device. In order to revoke the registration, the admin will need to wipe the entire Chrome OS device.

Registered profiles and devices check for policy changes periodically (every 3 hours by default). In some cases, the server pushes policy changes to the client without waiting for Chrome's periodic check. Unregistered profiles check whether a policy has been turned on for their domain each time Chrome starts up.

The policy list contains details about the types of configurations that are available via Cloud Policy.

Lite Mode

If you enable Lite Mode, Chrome will send your traffic through Google's optimizing proxy servers. This option reduces the amount of data downloaded and speeds up your page loads. This feature was previously known as “Data Saver”.

Most of the time, only your HTTP traffic is transparently proxied, and you won't notice any changes to the page. However, if Chrome anticipates the page will load especially slowly, both HTTP and HTTPS pages will be optimized to load faster. For HTTPS origins, the transcoded pages are served from a Google-owned domain instead of being transparently proxied. Because these pages are served from a Google-owned domain instead of the original domain, Chrome will not send any origin-scoped information (e.g., cookies or data from local storage) for the original domain to Google, and Google cannot set any origin-scoped information for the original domain in Chrome. Pages loaded in Incognito are never proxied or optimized by Lite Mode.

Additionally, when you enable Lite Mode, Chrome may share the URLs and usage and performance statistics of the websites you visited with Google in order to identify the websites that load slowly and improve their performance.

Request URLs are logged, but Cookie and If-None-Match headers are stripped from the logs (and cookies are never seen in the case of HTTPS pages). Additionally, the content of proxied pages is cached but not logged. The logs are not associated with your Google Account, and the entire log entry is removed within 14 days. These logs are also governed by standard Google search logging policies.

Google uses the logged and cached data to improve both Lite Mode and Safe Browsing; for example, more effective optimizations can be uncovered by analyzing timing data for pages loaded through the proxy service, and malware can be detected more rapidly by analyzing response data in realtime.

Your IP address is forwarded to the origin HTTP server via an X-Forwarded-For header, in accordance with the HTTP standard. The Lite Mode service is a transparent proxy, *not* an anonymization service.

By default, the connection between the browser and the Lite Mode proxy is over an encrypted channel. However, a network administrator can disable the use of an encrypted channel to Lite Mode.

To further improve loading performance for Lite mode users, if you have the “Preload pages for faster browsing and searching” setting enabled, Chrome may prefetch search result links found on the Google Search page. Four mechanisms preserve user privacy for these prefetches:

- Prefetching is disabled if Chrome has a cookie for the domain.
- Passive fingerprinting surfaces such as User-Agent are bucketed or set to fixed values.
- Prefetches are tunneled through a CONNECT proxy operated by Google, and only HTTPS links are prefetched. Consequently, the TLS connection is established between Chrome and the origin so the proxy server cannot inspect the traffic, and requests to the origin come from a Google IP instead of the user's IP. Google only learns about the destination domain that will be prefetched, which Google already knows as it generated the Search results page.
- Prefetched resources and cookies set by the prefetched domain are only persisted when you click the search result and visit the prefetched domain.

Using Chrome with a kid's Google Account

Case 4:20-cv-03664-YGR Document 528-7 Filed 04/05/22 Page 36 of 246

Chrome for Android offers features to be used when signed in with a kid's Google Account and automatically signs in a kid's account if they've signed into the Android device. Chrome uses the Sync feature to sync settings configured by parents to the kid's account. You can read about how Sync data is used in the Sign in section of this Whitepaper.

The collection and use of Chrome data in association with a kid's Google Account are governed by the Google Family Link - Children's Privacy Policy.

In order for the configured settings to apply to a kid's account, Chrome does not support the following features for a kid's Google Account: signing out of Chrome, Incognito mode, and deleting browsing history from within Chrome. Browsing history can still be removed in the Chrome section of the Google Dashboard.

By default, first party cookie blocking is disabled when Chrome is signed in with a kid's account. Parents can go to chrome.google.com/manage/family to allow their kids to block first party cookies. However, blocking cookies signs kids out of Google web products such as Google Search or YouTube and therefore prevents these products from providing any features designed for kids' Google Accounts.

When Chrome is used with a kid's Google Account, information about the kid's requests to access blocked content is sent to Google and made visible to the kid's parent(s) on chrome.google.com/manage/family and in the Google Family Link app. If the kid's browsing mode is set to "Try to block mature sites", Chrome will send a request to the Google SafeSearch service for each navigation in order to block access to sites that have been classified as containing mature content.

Incognito and Guest Mode

Incognito mode in Chrome is a temporary browsing mode. It ensures that you don't leave browsing history and cookies on your computer. The browsing history and cookies are deleted only once you have closed the last incognito window. Incognito mode cannot make you invisible on the internet. Websites that you navigate to may record your visits. Going incognito doesn't hide your browsing from your employer, your internet service provider, or the websites you visit.

Browsing as a Guest in Chrome allows you to use somebody else's computer without modifying their profile. For example, no bookmarks or passwords get stored on their computer. Note that Guest mode does not protect you for example, if the computer you are using is infected by a keylogger that records what you type.

iOS 8 and Mac OS X Yosemite Handoff Support

While browsing in a standard (i.e. non-Incognito) session, Chrome will share your current URL with iOS 8+ to support the Handoff feature that was added in OS X Yosemite. This information is only sent to Apple devices that are paired with your iOS device, and the data is encrypted in transit.

More information is available at Apple Support, Apple Developers, and in the Apple iOS Security Guide. Chrome support for this feature can be disabled in Chrome settings.

Security Key

A FIDO U2F Security Key provides a non-phishable credential which can be used to authenticate a user. This mitigates the risk of various kinds of man-in-the-middle attacks in which websites try to steal your password and use it later.

To prevent abuse, a website is required to be delivered over a secure connection (HTTPS), and to register the security key before it can be used for identification. Once a website is registered with a specific security key, that security key will provide a persistent identifier, regardless of which computer it is plugged into, or whether you're in incognito or guest mode, but you must physically interact with the security key to give a website access to an identifier (by, for example, touching it, or plugging it in).

Physical Web

The Physical Web lets you see a list of URLs being broadcast by objects in the environment around you. Google Chrome looks for Physical Web devices with Bluetooth Low Energy beacons that are broadcasting URLs using the Eddystone protocol. Bluetooth signals can be received from 90 feet away or more, depending on signal strength and the user's environment (although the range is often much shorter, due to obstacles and signal noise). If the Physical Web feature is enabled, Chrome sends detected URLs to Google's Physical Web Service (PWS) via a cookieless HTTPS request. For each URL, the PWS obtains the title of the web page, filters out unsafe results, and returns a ranking based on non-personalized signals about the quality and relevance of the web page.

The Physical Web feature is available on Chrome on iOS and Android. Users will need to turn on Bluetooth to use the feature.

If Android users have location settings enabled on both their device and in Chrome, they will receive a notification the first time they are near a beacon that will give them the option to turn on the Physical Web feature. This beacon's URL is not sent to Google's PWS unless the Physical Web feature is enabled. Users can also enable (or disable) the feature in the Privacy settings. Once a user enables the feature, Chrome scans for nearby devices for a few seconds each time the user unlocks the mobile device in use and sends them to the PWS in order to obtain more information about the beacon. The user receives a silent notification when Chrome finds a nearby URL.

On iOS devices, users can [enable](#) (or disable) the feature in the Privacy settings or by adding the Chrome widget to their Today view in the notification center. Additionally, the feature is automatically enabled for users who have location enabled on their device, granted Chrome the location permission, and have granted Google the geolocation permission. Chrome scans for nearby devices whenever it is open in the foreground. When Chrome finds nearby URLs, users will see them as omnibox suggestions. Additionally, Chrome scans for nearby devices for a few seconds when the Today widget is displayed in the notification center.

Bluetooth

Google Chrome supports the [Web Bluetooth API](#), which provides websites with access to nearby [Bluetooth Low Energy devices](#) with your consent.

Chrome does not let any page communicate with a device unless you explicitly consent. When a web page asks to pair with a device, Chrome will ask you to choose which device the web page should access, if any. Selecting a device for one page does not give other pages access to the device you have chosen, and does not allow that page to access other devices. Currently, permission for a page to communicate with a device is usually revoked when the page is reloaded, and is always revoked when Chrome is restarted.

Chrome data that Android sends to Google

The data collection and usage described in this section is handled by Android and governed by the [Google Privacy Policy](#).

If the Android Backup Service is enabled on your device, some of your Chrome preferences will be saved and stored on Google servers. For Nexus and Android One devices, it is described under “Back up your data and settings with Android Backup Service” in [this article](#). For other Android devices, you may be able to find help by looking up your device on [this page](#). When setting up a new Android device, you may request that it copies the preferences from a previously set up device. If you do so, Android may restore backed up Chrome preferences when Chrome is first installed. The new device only copies the preferences if automatic restore is enabled (see “Restore your data and settings” in [the same article](#)), Chrome was signed into an account when the backup was made, and the new Android device is signed into that same account.

Chrome’s backup data for a particular device may also be restored if you uninstall and then later re-install Chrome on that device. This will only happen if automatic restore is enabled and the device is signed into the account that Chrome was signed into when the backup was made.

Integration with Digital Wellbeing

If you opt-in to see sites you have visited and set site timers in the Digital Wellbeing app on Android, Chrome will report which websites you’ve visited and the length of time spent in each of them to the app. Sites visited in incognito mode will not be reported to the Digital Wellbeing app.

To continually improve the experience of Digital Wellbeing, the app will share with Google the websites that you set a timer on and how long you have visited them.

You can opt out of this feature in the Digital Wellbeing app or in Chrome’s privacy settings anytime.

Follow us



Chrome Family

Other Platforms

Chromebooks

Chromecast

Chrome Cleanup Tool

Enterprise

Download Chrome
Browser

Chrome Browser for
Enterprise

Chrome Devices

Chrome OS

Google Cloud

Google Workspace

Education

Google Chrome Browser

Devices

Web Store

Dev and Partners

Chromium

Chrome OS

Chrome Web Store

Chrome Experiments

Chrome Beta

Chrome Dev

Chrome Canary

Stay Connected

Google Chrome Blog

Update Chrome

Chrome Help

Chrome Tips

EXHIBIT 15
Redacted in its
Entirety

EXHIBIT 16
Redacted in its
Entirety

EXHIBIT 17
Redacted in its
Entirety

EXHIBIT 18
Redacted in its
Entirety

EXHIBIT 19
Redacted in its
Entirety

EXHIBIT 20
Redacted in its
Entirety

EXHIBIT 21
Redacted in its
Entirety

EXHIBIT 22
Redacted in its
Entirety

EXHIBIT 23
Redacted in its
Entirety

EXHIBIT 24
Redacted in its
Entirety

EXHIBIT 25
Redacted in its
Entirety

EXHIBIT 26
Redacted in its
Entirety

EXHIBIT 27
Redacted in its
Entirety

EXHIBIT 28
Redacted in its
Entirety

EXHIBIT 29
Redacted in its
Entirety

EXHIBIT 30
Redacted in its
Entirety

EXHIBIT 31
Redacted in its
Entirety

EXHIBIT 32

quinn emanuel trial lawyers | san francisco

50 California St., 22nd Floor, San Francisco, California 94111 | TEL (415) 875-6600 | FAX (415) 875-6700

WRITER'S DIRECT DIAL NO.
(415) 875-6426

WRITER'S INTERNET ADDRESS
jonathantse@quinnemanuel.com

January 25, 2021

VIA E-MAIL

Beko Reblitz-Richardson
Boies Schiller Flexner LLP
44 Montgomery St., 41st Floor
San Francisco, CA 94104

Re: *Brown, et al. v. Google LLC* – U.S. District Court, Northern District of California, San Jose Division: Case No. 5:20-cv-03664-LHK-SVK

Dear Counsel,

Pursuant to the First Modified ESI Protocol (Dkt. 91), please find attached Google's ESI production custodians (Appendix A). We look forward to discussing during our meet and confer tomorrow.

Sincerely,

/s/ Jonathan Tse

Jonathan Tse

APPENDIX A

CONFIDENTIAL

Brown v. Google

Case No. 5:20-cv-03664-LHK-SVK

ESI Production Custodian Chart

Name	Title	General Duties
Berntson, Glenn	Engineering Director	Engineering Director leading Ad Manager.
Bhatnagar, Deepti	Product Manager	Product Manager Lead for Ad Manager.
Borsay, Sabine	Product Manager	Product Manager leading Chrome Identity and Chrome Incognito.
Fair, Greg	Product Manager	Product Manager in Privacy & Data Protection Office for Fundamental Notices & Consents, which involves running large scale notice and consent campaigns at Google.
Harris, Helen	Research Manager	Research Manager for Chrome UX (User Experience) Research.
Mardini, Abdelkarim	Product Manager	Group Product Manager of Chrome Trust & Safety Team.
Schuh, Justin	Director	Director leading Chrome Trust & Safety and Privacy Sandbox.
Stone, Dan	Product Manager	Product Manager for Google Analytics managing publisher websites' use of Google Analytics.
Svitkine, Alexei	Software Developer	Technical Lead for the Chrome Metrics Team, which provides Chrome developers with tools to find insights into the user experience.
Wright, Keith	Software Engineer	Software Engineer managing Google Publisher Tagging.

EXHIBIT 33
Redacted Version of
Document Sought to
be Sealed

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY

quinn emanuel trial lawyers | washington, dc

1300 I Street NW, Suite 900, Washington, District of Columbia 20005-3314 | TEL (202) 538-8000 FAX (202) 538-8100

WRITER'S EMAIL ADDRESS

josefansorge@quinnemanuel.com

February 5, 2021

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY

VIA E-MAIL

BRICHARDSON@BSFLLP.COM

Beko Reblitz-Richardson
Boies Schiller Flexner LLP
44 Montgomery St.
41st Floor
San Francisco, CA 94104
Phone 415 293 6804

Re: ***Chasom Brown, et al., v. Google LLC, Case No. 5:20-CV-03664-LHK***

Dear Counsel:

I write on behalf of Google LLC (“Google”) in response to your January 19, 2021 letter regarding paragraph 4(a) of the ESI Order.

Plaintiffs allege they understood certain Google disclosures to mean that when they browsed the Internet in “private browsing” mode while not logged-in to their Google Account, Google would not receive the basic browsing data it collects on behalf of websites to provide Google Analytics and Ad Manager web-services. Thus, Plaintiffs’ claims turn on the narrow issue of how Google’s Privacy Policy and other disclosures may reasonably be interpreted.

Google is fulfilling its preservation obligations. Among other information, Google is preserving data related to the Google Accounts you have indicated are associated with the Named Plaintiffs. That data includes Plaintiffs’ Google Account name, Google Account ID, date of account creation, email address, alternate email address, IP logs that contain IP addresses and User Agents, cookie values related to Plaintiffs’ sign-ins, and My Activity information which would include—depending on user settings and actions—URL information of sites visited and time stamps.

Plaintiffs now ask Google to suspend the regular retention policies of all logs that may record any data from users’ private browsing in the United States. Plaintiffs claim that “it appears

quinn emanuel urquhart & sullivan, llp

LOS ANGELES | NEW YORK | SAN FRANCISCO | SILICON VALLEY | CHICAGO | WASHINGTON, DC | HOUSTON | SEATTLE | BOSTON | SALT LAKE CITY
LONDON | TOKYO | MANNHEIM | HAMBURG | PARIS | MUNICH | SYDNEY | HONG KONG | BRUSSELS | ZURICH | SHANGHAI | PERTH | STUTTGART

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY

Google’s February 5, 2021 Ltr. to Plaintiffs’ Counsel

necessary to preserve all logs” of logged-in and logged-out users that may contain data generated during private browsing sessions “so that Plaintiffs can evaluate those logs and other data to assess the best way to identify private browsing mode users and the data collected from their private browsing.” Letter at 5. Google disagrees. Plaintiffs’ request is grossly disproportionate to the needs of the case.

Information About the Logs Implicated By Plaintiffs’ Preservation Demand

Plaintiffs’ preservation demand implicates certain Identity logs, Analytics logs, and Display Ad logs. These logs contain information about user website visits. The Identity logs are linked to a user’s Google Account. The Analytics and Display Ad logs are of two types: either linked to a user’s Google Account (“Google Account keyed logs”) or linked to another identifier (“non-Google Account keyed logs”).

The log data is not reasonably limited by geographic region, by browser, or by browser mode). For that reason, Plaintiffs’ preservation request sweeps in a plethora of data for millions of individuals who are not putative class members. Moreover, the data in Google Account-keyed logs is subject to user controls. At the “My Activity” page, a user can set auto-deletion periods (3 months, 18 months, or 36 months), as well as review and delete individual entries of the data Google received when that user visited a website that used Google services. Those deletion requests are then propagated to the relevant Google Account keyed logs. In addition, the data in the Google Analytics logs is subject to the control of the Google Analytics’ customers on whose behalf Google collects the data.

Suspending the Retention Periods On These Logs Is Not Feasible

First, the sheer size of these logs makes Plaintiffs’ demand unworkable. These logs cover [REDACTED], and include data reflecting the activity of [REDACTED] of users, many of whom are not putative class members. Google estimates that suspending preservation of these logs—even if possible—would result in an additional [REDACTED] of data needing to be stored every thirty days.¹ That would mean that to satisfy Plaintiffs’ demand, every thirty days Google would need to add the equivalent of [REDACTED] laptops to its server space. Further, any suspension of the retention periods is complex—it is not as simple as an on/off switch. The effort involved with suspending the retention periods would entail months of work by teams of engineers. Further, managing this volume of data for the indefinite duration of the litigation would involve hundreds, if not thousands, of hours of engineering work and cost millions of dollars in storage costs alone—which would continue increasing throughout the life of the case. By way of example, the size of one [REDACTED] log for a single 30 day period is [REDACTED]. It defies reason to believe that Plaintiffs will spend the resources necessary to host, manage, review, and actually use in this litigation many multiples of that amount of data.

¹ It would take [REDACTED] to download [REDACTED] over a high-speed gigabit Internet connection.

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY

Google’s February 5, 2021 Ltr. to Plaintiffs’ Counsel

Simply put, such substantial costs just for preservation are grossly disproportionate to the needs of a case in which Plaintiffs allege no monetary harm, and where they have yet to articulate a need for all of the data at issue. *See Lord Abbett Mun. Income Fund, Inc. v. Asami*, 2014 WL 5477639, at *3 (N.D. Cal. Oct. 29, 2014) (stating “[t]his district recognizes that the proportionality principle applies to the duty to preserve potential sources of evidence” and holding that requiring a party to continue to pay \$500 per month to store computers outweighed the likely benefit of maintaining the computers.) As explained above, the logs Plaintiffs demand Google preserve are overly inclusive and implicate a substantial amount of information that is irrelevant here because not limited to data associated with users in private browsing mode. A party need not preserve data beyond what is truly “needed to prosecute th[e] case.” *FTC v. DirecTV, Inc.*, 2016 WL 7386133, at *5 (N.D. Cal. Dec. 21, 2016) (no prejudice where although preservation was not perfect, it was sufficient for stated need). Since there is no reason to think that even a fraction of this data will ever be used in litigation, Plaintiffs’ demand that it all be preserved is disproportionate to the needs of the case. N.D. Cal. Guideline 1.03 (proportionality standard set forth in Rule 26(b)(1) applies to preservation of information); see also Fed. R. Civ. P. 37(e) Adv. Comm. Notes (2015) (“[P]erfection in preserving all relevant electronically stored information is often impossible.”). Preservation should not be required here because it is unworkable and Plaintiffs have failed to articulate a need for the information.

The authorities you cite are unavailing because none concerns a preservation burden of even remotely similar magnitude. *See Bright Sols. for Dyslexia, Inc. v. Doe 1*, 2015 WL 5159125, at *3 (N.D. Cal. Sept. 2, 2015) (court-ordered preservation was limited to ***data associated with one Google Account***); *In re Napster, Inc. Copyright Litig.*, 462 F. Supp. 2d 1060, 1067 (N.D. Cal. 2006) (case decided prior to 2015 amendment to the Federal Rules of Civil Procedure introduced “proportionality test”); *National Ass’n of Radiation Survivors v. Turnage*, 115 F.R.D. 543, 557–58 (N.D. Cal. 1987) (same).

Second, the data Plaintiffs are asking Google to preserve is not necessary to Plaintiffs’ claims and therefore not proportional to the needs of the case. Plaintiffs allege that Google identifies and tracks users when they are logged ***out*** of their Google Accounts and in private browsing mode. Compl. ¶ 192 (limiting class to users who browsed in private mode while “not logged into their Google account”). Google has explained that its systems are designed such that data generated by users who are logged out is not linked—or reasonably linkable—to those individuals. Google understands that Plaintiffs wish to test this proposition, but to do so, Plaintiffs do not require—and are not entitled to—all of Google’s website activity data that may be associated with US-based users. It is sufficient for Google to produce information sufficient to show that the data at issue is not linked, and not reasonably linkable, to individual users. Plaintiffs’ requested log data preservation is neither necessary for—or proportional to—showing the data at issue is not reasonably linked to individual users.

Nor would these logs help Plaintiffs identify purported class members. As Google has explained during the meet and confer process, Google does not maintain information to identify whether a user was private browsing. Therefore, contrary to your implicit assumption, there are no

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY

Google’s February 5, 2021 Ltr. to Plaintiffs’ Counsel

separate logs of private browsing data that Google then “aggregate[s]” with non-private browsing data. Ltr. at. 3. For the reasons explained in detail in our January 21, 2021 letter, Plaintiffs’ speculation about how they might be able to identify private browsing data in these logs and then link that data to specific users is unfounded and wrong. Ansorge 1/21/21 Ltr. To Richardson at 3-4.

Google is not required to fulfill Plaintiffs’ unreasonable preservation demand simply because Plaintiffs assert—without basis—that all log data, including those from logged-in users, are relevant. *See Am. LegalNet, Inc. v. Davis*, 673 F. Supp. 2d 1063, 1073 (C.D. Cal. 2009) (refusing to issue a preservation order where a preservation of “all information” relevant to the complaint as unduly burdensome); *see also Pettit v. Smith*, 45 F. Supp. 3d 1099, 1107 (D. Ariz. 2014) (“Whether preservation or discovery conduct is acceptable in a case depends on what is *reasonable*, and that in turn depends on whether what was done—or not done—was *proportional* to that case and consistent with clearly established applicable standards.”).

Third, the preservation you demand is unfeasible because it would undermine Google’s compliance with its legal obligations, its public commitment to user privacy, and compliance with its contractual obligations. Google’s procedures and processes are designed to comply with a complex array of applicable data privacy laws and regulations. Similarly, its retention periods and data privacy policies are carefully crafted to abide by Google’s legal obligations under laws in various jurisdictions in which it operates, including EU General Data Protection Regulation 2016/679, the California Consumer Privacy Act (CCPA), and Lei Geral de Proteção de Dados (LGPD). The retention policies at issue here reflect the requirements in these laws and regulations. The logs record data not limited by geographic region, by browser, or by browser mode (synced versus without sync enabled) and therefore implicate data for millions of individuals who are not putative class members. Google’s preservation obligation is not so broad as to compel it to put aside its obligations to respect users’ deletions and our data retention policies for data beyond what is strictly necessary to the litigation.

Beyond its compliance obligations, Google constantly strives to implement strong privacy protections that reflect additional guidance of data protection authorities. Suspending the ability of all U.S.-based users to control the data associated with their accounts would cause Google to run against its representations to users, and is inconsistent with Plaintiffs’ ostensible goal of preserving users’ privacy and control over their data. Similarly, Google maintains and processes data it receives through Google Analytics on behalf of the websites that use Google Analytics. Those websites, just like Google users, have the ability to set retention periods and delete data. Suspending the ability of all Analytics customers—whose websites may have been visited by users in private browsing mode—to delete data that Google stores on Analytics customers’ behalf is unduly burdensome, not proportional to the needs of the case and may be inconsistent with our contractual obligations.

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY

Google’s February 5, 2021 Ltr. to Plaintiffs’ Counsel

Google’s Proposal

To resolve this preservation dispute, Google is prepared to preserve data associated with each Plaintiff’s Google Account(s) as recorded in the Identity logs and produce information sufficient to show that the information at issue is not linked, and not reasonably linkable, to specific users.

* * * *

We look forward to continuing to work with Plaintiffs to address and resolve any issues related to discovery in this matter.

Sincerely,

QUINN EMANUEL URQUHART & SULLIVAN, LLP

/s/ Josef Ansorge
Josef Ansorge

cc (via email):
Mark C. Mao, Esq.
Sean P. Rodriguez, Esq.
James Lee, Esq.
Rossana Baeza, Esq.
William S. Carmody, Esq.
Shawn Rabin, Esq.
Steven M. Shepard, Esq.
John A. Yanchunis
Ryan J. McGee

EXHIBIT 34
Redacted Version of
Document Sought to
be Sealed



July 16, 2021

SENT VIA EMAIL

QUINN EMANUEL URQUHART & SULLIVAN, LLP

Diane M. Doolittle
(dianedoolittle@quinnemanuel.com)
Thao Thai (thaothai@quinnemanuel.com)
555 Twin Dolphin Drive, 5th Floor
Redwood Shores, CA 94065

Andrew H. Schapiro
(andrewschapiro@quinnemanuel.com)
191 N. Wacker Drive, Suite 2700
Chicago, IL 60606

Stephen A. Broome
(stephenbroome@quinnemanuel.com)
Viola Trebicka
(violatrebicka@quinnemanuel.com)
865 S. Figueroa Street, 10th Floor
Los Angeles, CA 90017

William A. Burck
(williamburck@quinnemanuel.com)
Josef Ansorge
(josefansorge@quinnemanuel.com)
1300 I Street, N.W., Suite 900
Washington, D.C. 20005

Jonathan Tse
(jonathantse@quinnemanuel.com)
50 California Street, 22nd Floor
San Francisco, CA 94111

Jomaire Crawford
(jomairecrawford@quinnemanuel.com)
51 Madison Avenue, 23rd Floor
New York, NY 10010

**Re: *Chasom Brown, et al., v. Google LLC*, Case No. 5:20-cv-03664-LHK
Google Custodians and Searches**

Dear Counsel,

I write as a follow up to our June 22 letter regarding custodians and searches.

As discussed, Plaintiffs have been reviewing the documents Google produced on June 18, for the first 17 custodians, to identify additional custodians and searches.

Based on that ongoing review, and in addition to the individuals we previously proposed, Plaintiffs have identified a number of other Google employees who should be included as document custodians in this case and certain additional relevant searches.

Included in this letter is a summary of the reasons why Google should include these additional custodians plus specific searches for each of those custodians. We also include in this


BOIES SCHILLER FLEXNER LLP



CONTAINS INFORMATION FROM DOCUMENTS
PRODUCED BY GOOGLE AND DESIGNATED BY
GOOGLE AS PROTECTED INFORMATION

Google Counsel
July 16, 2021
Page 2

letter, as discussed previously, proposed additional searches for the current custodians and searches for the other proposed additional custodians. We already proposed searches for Mr. Liao, and we are waiting for your response to that proposal.

Please respond to this letter in writing by July 21, so that we can then meet and confer next week regarding these issues. Pursuant to the Court's June 30 order (Dkt. 209), the parties will need to brief any remaining disputes with the August 2 submission.

Plaintiffs are continuing to review Google's productions, and Plaintiffs reserve the right to seek the additional of other custodians and searches.

I. Additional Custodians

Based on our ongoing review of the documents produced by Google and other sources, Plaintiffs identify the following additional custodians with specific proposed searches for each person. Please let us know by July 21 whether Google agrees to add any or all of these individuals and, if so, whether Google will agree to these proposed searches. To the extent Google is unwilling to add any of these individuals and/or searches, please provide us with hit counts.

1. **Alex Ainslie.** Already a custodian in *Calhoun*, documents produced by Google in this case establish that he should also be a custodian in this case. For example, Mr. Ainslie's name is the first name listed on the Q3 2019 "Privacy-Focused Chrome" presentation, which (among other things) discusses the possibility of blocking third-party cookies "by default" in Incognito mode "to measure impact" and the possibility of "[a]ligning users['] expectations of Incognito with what it [Incognito] actually does" such as by adding features such as [REDACTED]. GOOG-BRWN-00165067; *see also* GOOG-BRWN-00165068 (discussing how "'Guest Mode'/'Temporary Mode' doesn't imply anonymity towards websites, Google and ISP and seems more true to what Incognito does today."). This document also discusses the "promise" of anonymity with Incognito. GOOG-BRWN-00165177. Mr. Ainslee is also identified as one of the contributors for a "Chrome Browser: 2019+ Strategy" document, which notes Google's intent to "[a]ddress known problems of Incognito." GOOG-BRWN-00139753. In July 2020, Mr. Mardini sent an email to the Chrome Trust & Safety team announcing changes to Chrome with 3rd-party cookie-blocking in Incognito, and he identified Mr. Ainslie as part of the "Leadership" with that effort. GOOG-BRWN-00189933. In May 2020, Mr. Ainslie also referenced certain Incognito "histograms" (GOOG-BRWN-00233108) and the roll-out of [REDACTED]. GOOG-BRWN-00181901; *see also* GOOG-BRWN-00050100 (Mr. Ainslie comments on modifying Incognito to provide for "3rd party cook[ie] blocking" and considering impact on publishers). Mr. Ainslee was also involved in changes to the Incognito NTP (GOOG-BRWN-00392367) and sent an email titled "Incognito Imprecision" that was critical of Google's public statements regarding Incognito. GOOG-BRWN-00184110. Mr. Ainslee very clearly had (and likely still has) a key role in terms of Google's Incognito efforts, and [REDACTED] included as a custodian.



CONTAINS INFORMATION FROM DOCUMENTS
PRODUCED BY GOOGLE AND DESIGNATED BY
GOOGLE AS PROTECTED INFORMATION

Google Counsel
July 16, 2021
Page 3

Plaintiffs propose the following searches for Mr. Ainslie:

- Incognito¹
- inPrivate
- Private! /3 (brows! OR mode)
- OTR OR (off /3 record)
- [REDACTED] OR [REDACTED]
- Histogram!
- (third OR 3rd OR 3d) /3 cookie!
- [REDACTED] OR [REDACTED] OR [REDACTED] OR [REDACTED] OR [REDACTED]

2. **Arne de Booj.** Mr. de Booj has direct personal involvement with Google projects and efforts focused on Incognito, control, transparency, consent, and other relevant issues. One document indicates, for example, that Mr. de Booj stated (correctly) that “[t]here does not seem to be a clear understanding of what incognito does to data collection and who can see what information.” GOOG-BRWN-00164006. Mr. de Booj also sent an email referencing [REDACTED] and asking whether “Chrome Incognito” was interested in “participating in a research immersion” to “learn about Incognito user needs & perceptions” where “consent” would be a topic. GOOG-BRWN-00182236. He also sent an email regarding the PDPO “privacy in context” efforts, focusing on “consent & transparency” and Google’s “transparency & control efforts.” GOOG-BRWN-00220475. He was identified as one of the “Owners” for a project focused on “consent patterns, including to assess user comprehension and user feedback to messaging.” GOOG-BRWN-00222188. Mr. de Booj was also included in discussions regarding Incognito users, including user consent and understanding. *See* GOOG-BRWN-00406075–76 (discussing “what we know about Incognito users” and noting that “Incognito mode is used by [REDACTED] of Chrome users, and [REDACTED] use it at least once per week” and that “[u]sers overestimate the protections that Incognito provides”); GOOG-BRWN-00246549 (discussing studies focused on Incognito but having participants “look at Incognito before asking about expectations for an UnAuth consent”); GOOG-BRWN-00059467 (noting that “incognito also has some overlap with UnAuth”); GOOG-BRWN-00176824, -00176828 (discussing research relating to signed-out users and users that do not use their Google Account and noting that “every incognito window gets a new zwieback”); GOOG-BRWN-00177213 (discussing research involving “incognito with a combined consent”).

Plaintiffs propose the following searches for Mr. de Booj:

- Incognito

¹ Please confirm that “Incognito” from prior searches would have captured “Incognito++.” Otherwise, Plaintiffs request to change the search term “Incognito” to “Incognito!”



CONTAINS INFORMATION FROM DOCUMENTS
PRODUCED BY GOOGLE AND DESIGNATED BY
GOOGLE AS PROTECTED INFORMATION

Google Counsel
July 16, 2021
Page 4

- inPrivate
- Private! /3 (brows! OR mode)
- Consent!
- Unauth! OR “signed out”
- [REDACTED] OR [REDACTED] OR [REDACTED] OR [REDACTED] OR [REDACTED]
- Anonym! OR pseudonymous

3. **Benjamin Poiesz.** During the class period, in 2019, Mr. Poiesz sent an email proposing that Google change Incognito so that it would actually (as promised) “provide anonymity.” GOOG-BRWN-00403704. He has also proposed consideration of changing Google’s business model to a “[r]ev share back to users” based on their data. GOOG-BRWN-00405767. On February 12, 2021, Ane Aranzabal added Mr. Poiesz to an email exchange “for Incognito/PPN” in connection with a “Sundar presentation.” GOOG-BRWN-00220480. This document also discusses Google’s “transparency & control efforts” and the issue of “consent & transparency.” *Id.* Mr. Poiesz has also had a lead role with “PPN & Incognito” and efforts to “better understand rev impact.” GOOG-BRWN-00223134. In 2015, he was identified in connection with “Incognito-fest,” which focused on “the current state of Incognito and developing a shared understanding of where we are.” GOOG-BRWN-00184710. Based on these and other documents, Mr. Poiesz should be included as a custodian.

Plaintiffs propose the following searches for Mr. Poiesz:

- Incognito
- inPrivate
- Private! /3 (brows! OR mode)
- OTR OR (off /3 record)
- [REDACTED] OR [REDACTED]
- [REDACTED] OR [REDACTED] OR [REDACTED] OR [REDACTED] OR [REDACTED]
- rev! /3 (share OR impact)

4. **Breen Baker.** Mr. Baker has worked at Google since August 2011 as a Product Manager with Google Analytics.² Based on the documents Google produced for other custodians, it appears that Mr. Baker has in-depth knowledge about Google’s cross-device conversions and tracking. *See, e.g.,* GOOG-BRWN-00171370 (discussing Biscotti ID tying); GOOG-BRWN-00170140 (discussing linking of anonymous and user id). His documents are relevant in terms of

² <https://www.linkedin.com/in/breenbaker> [REDACTED]



CONTAINS INFORMATION FROM DOCUMENTS
PRODUCED BY GOOGLE AND DESIGNATED BY
GOOGLE AS PROTECTED INFORMATION

Google Counsel
July 16, 2021
Page 5

understanding Google's use of private browsing data in connection with various Google services and also potentially identifying class members.

Plaintiffs propose the following searches for Mr. Baker:

- Incognito
- inPrivate
- Private! /3 (brows! OR mode)
- Zw! OR biscotti OR cookie!
- conver! OR track!
- Anonym! OR pseudonymous OR unauth!

5. **Brad Townsend.** Already a custodian in *Calhoun*, Mr. Townsend appears to have deep and unique knowledge about Google's collection and tracking of data. For example, in an internal discussion, Dan Stone asks "what tests do we have to ensure that we don't accidentally set/collect the GA 1P cookies when analytics consent is disabled" and then defers that question to Mr. Townsend. GOOG-BRWN-00236984. Mr. Townsend then provided an explanation on how Google's "consent controls are focused on client storage, and we enforce that GA cookies are not read/written client side in the tagging code." *Id.* In a document called "Conversion Tracking in Firefox Private Browsing Mode," Google explains how Firefox's Private Browsing Mode blocks third-party cookies and "most background tracking pings," and therefore breaks Google's "conversion tracking and remarketing collection." GOOG-BRWN-0027314. The study's objective was to "[e]nable conversion tracking on Firefox in Private Browsing mode through a client side fix." *Id.* Mr. Townsend appears throughout the document as someone with knowledge about how to implement that study. See GOOG-BRWN-00027320–22.

Plaintiffs propose the following searches for Mr. Townsend:

- Incognito
- inPrivate
- Private! /3 (brows! OR mode)
- Firefox
- Zw! OR biscotti OR cookie!
- conver! OR track! OR remarket!
- Anonym! OR pseudonymous OR unauth!
- consent!

6. **Chetna Bindra.** Already a custodian in *Calhoun*, Ms. Bindra appears to have unique knowledge about Google's blocking of cookies and use of pseudonymous IDs. For example, she was involved in the launch of [REDACTED], Google's feature that "will start



CONTAINS INFORMATION FROM DOCUMENTS
PRODUCED BY GOOGLE AND DESIGNATED BY
GOOGLE AS PROTECTED INFORMATION

Google Counsel
July 16, 2021
Page 6

blocking third-party cookies in Incognito mode by default.” GOOG-BRWN-00173274–77. *See also* GOOG-BRWN-00062399 (discussing meeting with Ms. Bindra regarding [REDACTED] and “what mocks we can provide for the upcoming Sundar review,” and noting “concern” that Ms. Bindra shared a deck that “promises fundamental changes to Chrome’s Incognito mode”); GOOG-BRWN-00171653 (discussing “Ramp-up Plan for [REDACTED]”). In one Google document, Ms. Bindra expressed concern over a Google statement regarding how “user data associated with pseudonymous ID can be shared with advertising platforms while browsing the web, including which web pages are being visited,” which she described as “going to cause a firestorm.” GOOG-BRWN-00175635. She likely has documents relevant to Google’s tracking and cookie blocking efforts, including with Incognito.

Plaintiffs propose the following searches for Ms. Bindra:

- Incognito
- inPrivate
- Private! /3 (brows! OR mode)
- Zw! OR biscotti OR cookie!
- Anonym! OR pseudonymous OR unauth!
- [REDACTED] OR [REDACTED]

7. **Chris Palmer.** Mr. Palmer appears to have unique knowledge about user confusion regarding Incognito mode. Mr. Palmer’s name appears on the first page of a Google presentation titled “The Incognito Problem” that begins with the “key fact” that “Incognito confuses people” and then proposes solutions, such as “improv[ing] Incognito such that it provides more of what people (both mistakenly, and correctly) expect it does.” GOOG-BRWN-00140297–99, -00140316. In one internal email, Mr. Palmer notes that “[t]he phrase ‘Browse without a trail of cookie crumbs’ makes it sound like maybe Incognito doesn’t support cookies at all, or that it somehow exerts a Do not Track-like behavior on servers,” and is “all so imprecise.” GOOG-BRWN-00184109. Mr. Palmer advocated that Google should “abandon the Incognito name” because “[i]t’s not clear enough.” GOOG-BRWN-00167338. He noted that “I’ve already made my case (for 5 years now)” about this issue. *Id.*

Plaintiffs propose the following searches for Mr. Palmer:

- Incognito
- inPrivate
- Private! /3 (brows! OR mode)
- OTR OR (off /3 record)
- (User! OR people) /10 confus!
- Track!– [REDACTED] [REDACTED]



CONTAINS INFORMATION FROM DOCUMENTS
PRODUCED BY GOOGLE AND DESIGNATED BY
GOOGLE AS PROTECTED INFORMATION

Google Counsel
July 16, 2021
Page 7

- Cookie!

8. **David Monsees.** Already a custodian in *Calhoun*, the documents produced by Google establish that he should also be a custodian in this case. Not only did Google identify Mr. Monsees as its corporate representative regarding Google data logs in *Calhoun*, with many documents tied to him regarding those logs, he has been involved with various aspect of Incognito. For example, Sammit Adhya included him on an email regarding the June 2019 “Incognito Product Workshop” (GOOG-BRWN-00177764), and Mr. Monsees was identified as someone Rory McClelland should meet as the “PM lead for Footprints and very actively involved in Google’s overall privacy conversations.” GOOG-BRWN-00165704. Mr. Monsees also attended presentations and received emails relating to Sin Rastro and Incognito. GOOG-BRWN-00176982. In July 2020, Mr. Mardini sent an email to the Chrome Trust & Safety team announcing changes to Chrome with 3rd-party cookie-blocking in Incognito, and he identified Mr. Monsees as part of the team contributing to those Chrome-related efforts. GOOG-BRWN-00189933. In December 2020, Mr. Monsees was identified as one of the “Incognito PM Leads” and seeking information about “what it might mean to honor a user’s explicit request for privacy when they turn on Incognito mode.” GOOG-BRWN-00246045.

Plaintiffs propose the following searches for Mr. Monsees:

- Incognito
- inPrivate
- Private! /3 (brows! OR mode)
- [REDACTED] OR [REDACTED]
- [REDACTED] OR [REDACTED] OR [REDACTED] OR [REDACTED] OR [REDACTED]
- [REDACTED]
- “Sin Rastro”
- (user! OR people) /10 (privacy OR consent!)

9. **Deepak Ravichandran.** Already a custodian in *Calhoun*, the documents produced by Google establish that he should also be a custodian in this case. Mr. Ravichandran is Google’s principal engineer for Google Display Ads. He co-authored Google’s 2019 study on the effect of disabling third-party cookies on publisher revenue. GOOG-BRWN-00048286. This is an August 2019 public study where Google acknowledged that disabling third-party cookies would decrease publishers’ revenue by 52% average and 64% median—a serious threat to Google. Plaintiffs are entitled to documents relied on for that study and any communications Google employees and authors of competing studies that Mr. Ravichandran admittedly sought to contact. In another custodian’s production, one email from Mr. Ravichandran is captured referencing revenue impacts from third-party cookie blocking. GOOG-BRWN-00173681. This email pre-dates the May to August 2019 timeframe of that study. Plaintiffs served discovery requests for such documents (RFP Nos. 154, 155), wrote two letters to Google, and notified Google to



CONTAINS INFORMATION FROM DOCUMENTS
PRODUCED BY GOOGLE AND DESIGNATED BY
GOOGLE AS PROTECTED INFORMATION

Google Counsel
July 16, 2021
Page 8

explain the relevance and engage in any reasonable narrowing of the scope of documents sought, but Google has refused any production. Mr. Ravichandran is a senior Google employee for Google Display Ads and intimately involved in Google's determination of the impact blocking third party cookies would have on revenue.

Plaintiffs propose the following searches for Mr. Ravichandran:

- Incognito
- inPrivate
- Private! /3 (brows! OR mode)
- study AND (impact OR revenue OR sustain* OR advertis* OR publish*)
- SameSite
- nitish OR korula
- turtledove
- Zw! OR biscotti OR cookie!
- (user AND profile) AND (publish! OR remarket! OR rmktg)

10. **Dmitry Titov.** Mr. Titov is an Engineering Manager at Google with responsibilities tied to Chrome.³ Mr. Titov's documents are relevant in terms of understanding the development and history of Chrome and Google's data collection. *See, e.g.*, GOOG-BRWN-00109561 (discussion about Incognito profiles being passed to regular browsing mode); GOOG-BRWN-00130258 (changes to whitelists and functions capturing Incognito activity); GOOG-BRWN-00183781 (tracking system-level events while Incognito logged in UMA). Also, Mr. Titov was involved in discussions concerning the representations made in the Chrome Incognito splash screen and revisions detailing whether "private" was an appropriate representation. GOOG-BRWN-00131133. Further, Mr. Titov attended a 2017 Chrome Summit to discuss forthcoming changes to Chrome, including Incognito functions. GOOG-BRWN-00064645-48. Plaintiffs propose the following searches for Mr. Titov:

Plaintiffs propose the following searches for Mr. Titov:

- Incognito
- inPrivate
- Private! /3 (brows! OR mode)
- OTR OR (off /3 record)
- Zw! OR Biscotti OR cookie!

³ <https://www.linkedin.com/in/dmitrytitov/>



CONTAINS INFORMATION FROM DOCUMENTS
PRODUCED BY GOOGLE AND DESIGNATED BY
GOOGLE AS PROTECTED INFORMATION

Google Counsel
July 16, 2021
Page 9

- Anonym! OR pseudonymous OR unauth!
- Consent!
- Profile AND brows!
- UMA
- “Chrome Summit”

11. **Florian Uunk.** Mr. Uunk has been a software Engineer at Google since June 2012,⁴ and he appears to have unique knowledge regarding Incognito and the use of cookies in Incognito mode and other Incognito-related issues. For example, he managed projects involving third party cookie blocking in Incognito. GOOG-BRWN-00182804; *see also* GOOG-BRWN-00199591 (reviewing and approving changes regarding user control cookie blocking). In an internal discussion, Mr. Uunk “argue[s] against porting cookies across modes” because it “would be bad for privacy, and negatively surprising in many cases (why do I have stuff in my cart if I go incognito?, why is the stuff that I put in my cart in incognito mode there in regular mode?).” GOOG-BRWN-00183724. In June 2019, Mr. Uunk was chosen to “lead the development of Chrome Privacy features” such as “[redacted] and rethinking Incognito mode.” GOOG-BRWN-00167716. He has also been involved with reading Google histograms to analyze cases where the X-Client-Data header is not sent to Chrome, which includes when “[t]he user is in incognito mode.” GOOG-BRWN-00233093. Those efforts, including [redacted], are highly relevant in this case, and Mr. Uunk should be a custodian.

Plaintiffs propose the following searches for Mr. Uunk:

- Incognito
- inPrivate
- Private! /3 (brows! OR mode)
- OTR OR (off /3 record)
- Zw! OR biscotti OR cookie!
- Anonym! OR pseudonymous OR unauth!
- [redacted] OR [redacted]
- [redacted] OR [redacted] OR [redacted] OR [redacted] OR [redacted]

12. **Haskell Garon.** Mr. Garon is a Senior Product Manager for Google Cloud. GOOG-BRWN-00023916. According to his LinkedIn, he formerly served as the Senior Product

⁴ <https://de.linkedin.com/in/feuunk> [redacted] [redacted]



CONTAINS INFORMATION FROM DOCUMENTS
PRODUCED BY GOOGLE AND DESIGNATED BY
GOOGLE AS PROTECTED INFORMATION

Google Counsel
July 16, 2021
Page 10

Manager for Sellside Ad Platforms.⁵ Mr. Garon also spent six years managing a team of Product Managers responsible for the roadmap and strategy for third-party monetization of Google's publisher partners on Ad Manager, AdMob, and AdSense in Google's real-time ad exchange. Internal documents reflect that Mr. Garon has knowledge about Google's internal business process and monetization strategies. GOOG-BRWN-00242521. Mr. Garon's documents are relevant in terms of understanding Google's monetization of private browsing information.

Plaintiffs propose the following searches for Mr. Garon:

- Incognito
- inPrivate
- Private! /3 (brows! OR mode)
- (user OR data OR brows!) /25 (monetiz! OR profit! OR revenue)
- [REDACTED] OR [REDACTED] OR [REDACTED] OR [REDACTED] OR [REDACTED]

13. **Hyewon Jun.** Already a custodian in *Calhoun*, the documents produced by Google establish that Ms. Jun should also be a custodian in this case. For example, Ms. Jun has extensive discussions with Google employees regarding restrictions of Google's competitor's browsers like Mozilla Firefox and Microsoft Edge, and how their cookie blocking mechanisms would impact Google's advertising technologies and the substantial revenue Google derived (and continues to derive) from those technologies. GOOG-BRWN-000175565, GOOG-BRWN-00175673–75, GOOG-BRWN-00175744–45. Ms. Jun also was involved in discussions concerning Google's efforts to substitute its tracking technologies from cookies to pixels, and associated those cookie-less technologies with Google's existing user libraries. GOOG-BRWN-00173685; *see also* GOOG-BRWN-00175745. Ms. Jun was (and likely still is) very involved with Google's efforts to determine impacts on its revenue from industry-wide changes to cookie blocking before Google ever launched its own efforts, how to overcome those cookie blocking efforts via the use of cookie-less technologies, and how Chrome could enable those technologies, all of which ties into Google's efforts to continue tracking and monetizing the private browsing of Plaintiffs and putative class members in this case.

Plaintiffs propose the following searches for Ms. Hyewon:

- Incognito
- inPrivate
- Private! /3 (brows! OR mode)

⁵ <https://www.linkedin.com/in/haskellgaron/> [REDACTED] [REDACTED]



CONTAINS INFORMATION FROM DOCUMENTS
PRODUCED BY GOOGLE AND DESIGNATED BY
GOOGLE AS PROTECTED INFORMATION

Google Counsel
July 16, 2021
Page 11

- block! AND (impact! OR revenue! OR sustain! OR advertis! OR Mozilla OR Firefox OR Microsoft OR Edge)
- browser AND restrict* AND cookie!
- [REDACTED] OR [REDACTED] OR [REDACTED]
- Zw! OR biscotti OR cookie!
- PPID OR [REDACTED]
- [REDACTED] OR [REDACTED] OR [REDACTED] or [REDACTED] OR [REDACTED]

14. **Lorraine Twohill.** One document identifies Ms. Twohill as a member of a Google “privacy council” and includes her recommendation to “Make Incognito mode truly private,” such as by “turning cookie blocking on by default” and “adding cautionary language at moments like 3P sign-in.” GOOG-BRWN-00406067. She continued: “We are limited in how strongly we can market Incognito because *it’s not truly private*, thus requiring really fuzzy, hedging language that is almost more damaging.” *Id.* (emphasis added). She is also identified as responsible for “Privacy settings” at Google, with the goal to “improve the user experience” and increase “interactions with settings to achieve goals and/or better understand settings.” GOOG-BRWN-00210410; *see also* GOOG-BRWN-00203816 (identifying Ms. Twohill as one “Owner” of effort to making “Google’s approach to privacy clear”). Ms. Twohill is also apparently involved with [REDACTED] with Google acknowledging that “[i]t is no surprise that our users can’t explain what a Google Account is or what it would hold, if it can’t be seen OR is represented schizophrenically as is the case in many of our products today.” GOOG-BRWN-00155368. Despite other documents recognizing that Incognito is not private, this document references Incognito as part of Google’s “privacy controls” for users. *Id.* She was also identified as one of two owners of a “first meeting” with Mr. Pichai with “Incognito mode being one of the topics.” GOOG-BRWN-00184645; *see also* GOOG-BRWN-00185344 (“We’ve received feedback from Sundar and Lorraine that they’d like us to push to have a new Incognito icon ready for the IO announcement”). Ms. Twohill also sent a report on how Google “aggressively promoted Chrome” including demonstrating “Chrome’s incognito mode.” GOOG-BRWN-00229060–61. According to an April 2020 email concerning rebranding Incognito, that effort was “driven by Lorraine [Twohill] who told the PDPO steering committee that Incognito might need rebranding” while Mr. Pichai “didn’t want to put incognito under the spotlight.” GOOG-BRWN-00183088; *see also* GOOG-BRWN-00395008 (“We’ve received feedback from Sundar and Lorraine that they’d like us to push to have a new Incognito icon ready for the IO announcement.”). In May 2020, Ms. Twohill participated in a meeting concerning Incognito mode and “addressed the debate on naming.” GOOG-BRWN-00224176; *see also* GOOG-BRWN-00222952 (“Incognito: Teams in Chrome, Maps, YouTube, and Search have been working with Lorraine’s team and the PDPO on making incognito a more accessible and meaningful part of our privacy foundation”); GOOG-BRWN-00220453 (email concerning Incognito disclosures, with Google employee stating that draft was “overpromising for Chrome’s incognito mode” where also a copy “being reviewed with ... Loarraine”).

[REDACTED]



CONTAINS INFORMATION FROM DOCUMENTS
PRODUCED BY GOOGLE AND DESIGNATED BY
GOOGLE AS PROTECTED INFORMATION

Google Counsel
July 16, 2021
Page 12

Plaintiffs propose the following searches for Ms. Twohill:

- Incognito
- inPrivate
- Private! /3 (brows! OR mode)
- Block! /5 cookie!
- [REDACTED] OR [REDACTED]
- [REDACTED] OR [REDACTED] OR [REDACTED] OR [REDACTED] OR [REDACTED]

15. **Michael Kleber.** Already a custodian in *Calhoun*, the documents produced by Google establish that he should also be a custodian in this case. Mr. Kleber has been a software engineer at Google since 2007. He has communicated with Google employees about identification of Incognito sessions. GOOG-BRWN-00173637. Mr. Kleber is frequently tagged for discussions concerning Google's project [REDACTED], discussing cookie blocking, which is highly relevant in terms of understanding Google's Incognito-focused considerations and changes. GOOG-BRWN-00173305-06; GOOG-BRWN-00199741. Mr. Kleber was also designated as a speaker at Google's 2020 "Tagging Summit," specifically speaking about "The Future of Privacy." GOOG-BRWN-00174567. Further, Mr. Kleber was assigned projects concerning tagging for ad-conversion tracking. GOOG-BRWN-00144542. Mr. Kleber is also very familiar with tracking technologies, acknowledging "there are roughly zero non-Google companies whose tracking depends *only* on [third party] cookies," GOOG-BRWN-00183151, which demonstrates Mr. Kleber's knowledge concerning what other tracking technologies are used to identify individual across the internet.

Plaintiffs propose the following searches for Mr. Kleber:

- Incognito
- inPrivate
- Private! /3 (brows! OR mode)
- OTR OR (off /3 record)
- Zw! OR biscotti OR cookie!
- Anonym! OR pseudonymous OR unauth!
- Ad! AND conver! AND track!
- Chrome AND conver! AND measure!
- [REDACTED] OR [REDACTED] OR [REDACTED] OR [REDACTED] OR [REDACTED]

16. **Mike Pinkerton.** Mr. Pinkerton is a Senior Staff Software Engineer. GOOG-BRWN-00023911. "In 2018 Pink's team launched version 69 of Chrome iOS as part of the

[REDACTED]



CONTAINS INFORMATION FROM DOCUMENTS
PRODUCED BY GOOGLE AND DESIGNATED BY
GOOGLE AS PROTECTED INFORMATION

Google Counsel
July 16, 2021
Page 13

Chrome 10th Anniversary.”⁶ He has been involved in a Google project aiming to “resolve user misconceptions about what incognito mode offers and what id [sic] does not.” GOOG-BRWN-00181405. In one project regarding user “confusion” about “how to leave incognito,” Mr. Pinkerton suggested that Google instruct users that “[t]o leave incognito, swipe left.” GOOG-BRWN-00181584. He has also discussed how “Dark Mode” may have caused the “increase in Incognito usage.” GOOG-BRWN-00181580. In one document involving the “Chrome 2020 iOS Strategy – iOS Squad,” Mr. Pinkerton asked if “improved settings” are “on our 2020 roadmap” in response to a comment that Google “[i]nvest in a safe and private browsing experience for users (3d party cookie controls, Safe Browsing, improved privacy settings).” GOOG-BRWN-00182207. He has been involved in discussions concerning the development of Google’s toggle that purports to block third-party cookies during Incognito sessions. GOOG-BRWN-00182266. Mr. Pinkerton likely has relevant documents helpful to understanding users’ perceptions of Incognito mode and the development of [REDACTED].

Plaintiffs propose the following searches for Mr. Pinkerton:

- Incognito
- inPrivate
- Private! /3 (brows! OR mode)
- OTR OR (off /3 record)
- [REDACTED] OR [REDACTED]

17. **Nitish Korula:** Mr. Korula is Google’s Senior Staff Research Scientist for Google Ad Manager. He co-authored Google’s 2019 study on the effect of disabling third-party cookies on publisher revenue. GOOG-BRWN-00048286. This is an August 2019 public study where Google acknowledged that disabling third-party cookies would decrease publishers’ revenue by 52% average and 64% median—a serious threat to Google. Plaintiffs are entitled to documents relied on for that study and any communications Google employees and authors of competing studies that Mr. Korula admittedly sought to contact. GOOG-BRWN-00048288. In another custodian’s production, one email from Mr. Ravichandran—who was the other co-author of this study—is captured referencing revenue impacts from third-party cookie blocking. GOOG-BRWN-00173681. This email pre-dates the May to August 2019 timeframe of that study. Plaintiffs served discovery requests for such documents (RFP Nos. 154, 155), wrote two letters to Google, and have met and conferred with Google to explain the relevance and engage in any reasonable narrowing of the scope of documents sought, but Google has refused any production. Mr. Korula was also involved in two discussions about Google’s cryptic [REDACTED] [REDACTED] GOOG-BRWN-

⁶ https://en.linkfang.org/wiki/Mike_Pinkerton [REDACTED] [REDACTED]



CONTAINS INFORMATION FROM DOCUMENTS
PRODUCED BY GOOGLE AND DESIGNATED BY
GOOGLE AS PROTECTED INFORMATION

Google Counsel
July 16, 2021
Page 14

00171920; GOOG-BRWN-00171947. Mr. Korula is a senior Google employee for Google Ad Manager and is involved in Google's determination of the impact blocking third party cookies would have on revenue, and also building user profiles.

Plaintiffs propose the following searches for Mr. Korula:

- Incognito
- inPrivate
- Private! /3 (brows! OR mode)
- Zw! OR biscotti OR cookie!
- study AND (impact OR revenue OR sustain* OR advertis* OR publish*)
- SameSite
- [REDACTED]
- deepak OR ravichandran
- (user AND profile) AND (publish! OR remarket! OR rmktg)

18. **Othar Hansson.** Mr. Hansson appears to have a core role in Google's Privacy & Data Protection Office with personal involvement in numerous relevant Incognito-related projects and discussions. For example, in one email exchange, Mr. Hansson was questioned about Incognito, and he referenced certain "Incognito logs" kept by Google. GOOG-BRWN-00403751. Another Google employee responded: "The inconsistencies around incognito – to the point that even old-school Googlers often get them wrong are baffling to normal people." *Id.* He is also identified as one of the authors of "Data Transparency I/O Moment" that begins with the acknowledgement that "users do not have a clean mental model for the data that collects about them and how this data *is or is not* used across our products." GOOG-BRWN-00204424. That document identifies Incognito as "likely a billion-user product." On February 12, 2021, Ane Aranzabal added Mr. Hansson to an email exchange "for Incognito/PPN" in connection with a "Sundar presentation." GOOG-BRWN-00220480. This document also discusses Google's "transparency & control efforts" and the issue of "consent & transparency." GOOG-BRWN-00220475. In an email regarding the "Incognito definition," Mr. Hansson commented how "having a simple cross-Google mental model [for Incognito] has value to our users . . . but it's been hard to fully align existing product behavior into a more consistent state," also adding that "[i]t's definitely a bad experience resulting from lack of consistency across our products." GOOG-BRWN-00403753–53. Another document identifies Mr. Hansson as a co-lead of the "Strategic Programs" in Google's Privacy & Data Protection Office. GOOG-BRWN-00071584. Mr. Hansson has also had discussions regarding Google's ability "to distinguish between Incognito and non-Incognito sessions." GOOG-BRWN-00176433. Given his role and these and other documents, Mr. Hansson should be a custodian.

Plaintiffs propose the following searches for Mr. Hansson:

[REDACTED]



CONTAINS INFORMATION FROM DOCUMENTS
PRODUCED BY GOOGLE AND DESIGNATED BY
GOOGLE AS PROTECTED INFORMATION

Google Counsel
July 16, 2021
Page 15

- Incognito
- inPrivate
- Private! /3 (brows! OR mode)
- OTR OR (off /3 record)
- [REDACTED] OR [REDACTED]
- (user OR user's OR users OR data) /5 (transparen! OR control! OR consent!)
- [REDACTED] OR [REDACTED] OR [REDACTED] or [REDACTED] OR [REDACTED]

19. **Qi Dong.** Mr. Dong is a Software Engineer at Google. GOOG-BRWN-00023915. According to his LinkedIn, he worked as an Adwords Statistician for Google from June 2011 to November 2012.⁷ He focused on business analytics, products analytics, modeling, A/B testing and market research. Internal documents demonstrate that Mr. Dong has an expertise in display Ad publication strategies in the context of phasing out third party cookies. GOOG-BRWN-00173430. Internal documents also refer to Mr. Dong as a lead engineer on projects relating to Chrome. GOOG-BRWN-00161318. Mr. Dong likely has relevant documents concerning the technical aspects of Google's collection of private browsing information.

Plaintiffs propose the following searches for Mr. Dong:

- Incognito
- inPrivate
- Private! /3 (brows! OR mode)
- Zw! OR biscotti OR cookie!
- Anonym! OR pseudonymous OR unauth!

20. **Ramin Halavati.** Mr. Halavati has been a Senior Software Engineer at Google since August 2016,⁸ and has been dubbed the "Incognito expert." GOOG-BRWN-00182637. He has been involved, for example, in projects monitoring Incognito users. In one project involving the collection of "granular incognito usage states," Mr. Halavati agreed to consider metrics he described as "borderline," including the "[u]sage of Google products" and other data. GOOG-BRWN-0018539-10. In another project, Mr. Halavati described how "experiment data" was "a means of connecting regular and incognito sessions," and noted that "having more people in the experiment arms reduces the uniqueness of these users." GOOG-BRWN-00168793. Mr.

⁷ <https://www.linkedin.com/in/ilhyvmvm/>

⁸ <https://de.linkedin.com/in/ramin-halavati-81623b2b> [REDACTED]



CONTAINS INFORMATION FROM DOCUMENTS
PRODUCED BY GOOGLE AND DESIGNATED BY
GOOGLE AS PROTECTED INFORMATION

Google Counsel
July 16, 2021
Page 16

Halavati's documents are relevant in terms of understanding Google's collection and use of private browsing information from putative class members.

Plaintiffs propose the following searches for Mr. Halavati:

- Incognito
- inPrivate
- Private! /3 (brows! OR mode)
- (user OR user's OR users OR data) /s (monitor OR dashboard OR metric!)

21. **Rory McClelland.** Mr. McClelland appears to have been deeply involved with the Google [REDACTED] efforts, among other projects. In April 2020, he sent an email to Parisa Tabriz, Alex Ainslie, and Margaret Schmidt with a "roll-out plan for [REDACTED]" which was "the new feature in Incognito mode that will block third-party cookies by default." GOOG-BRWN-00181901-02. He is the one who wrote that [REDACTED]

[REDACTED] and that the "project impact is [REDACTED] (later corrected to [REDACTED]). *Id.* One email identifies Mr. McClelland as one of two "incognito experts." GOOG-BRWN-00182141. He was also involved with discussions regarding "enhanced incognito" with "strong anti-tracking enhancements" (GOOG-BRWN-00388456) and identified as one of two Chrome representatives for the June 2019 "Incognito Product Workshop" (GOOG-BRWN-00177764). In 2018, Mr. McClelland was told that he should "[o]wn Chrome's Incognito" and "determine how it should evolve in light of things like GDPR/ITP/etc." GOOG-BRWN-00165702.

Plaintiffs propose the following searches for Mr. McClelland:

- Incognito
- inPrivate
- Private! /3 (brows! OR mode)
- OTR OR (off /3 record)
- (third OR 3rd OR 3d) /3 [REDACTED] OR [REDACTED]
- [REDACTED] OR [REDACTED] OR [REDACTED] or [REDACTED] OR [REDACTED]
- track! OR antitrack! OR anti-track!

22. **Sree Pothana.** During his deposition, Glenn Bernston identified Sree Pothana as the person from Google Analytics he interviewed to prepare for the deposition. Bernston Tr. 331:17-331:23. In addition to his experience and knowledge with respect to Google Analytics, Mr. Pothana also appears to have in-depth knowledge about Google's use of identifiers (*e.g.*, GOOG-BRWN-00141411) and Google's logging practices (*e.g.*, GOOG-BRWN-00170877). In an internal document authored by Mr. Pothana, he describes the "[g]oal" of a project as [REDACTED]



CONTAINS INFORMATION FROM DOCUMENTS
PRODUCED BY GOOGLE AND DESIGNATED BY
GOOGLE AS PROTECTED INFORMATION

Google Counsel
July 16, 2021
Page 17

GOOG-BRWN-00141411. In a discussion about “Analytics Data Association,” Mr. Pothana states: [REDACTED] to mitigate the risk, but the risk is still there.” GOOG-BRWN-00170877. These are key issues in this case, and Mr. Pothana’s documents should be produced.

Plaintiffs propose the following searches for Mr. Pothana:

- Incognito
- inPrivate
- Private! /3 (brows! OR mode)
- Identifier! OR “user ID” OR gaia!
- Zw! OR biscotti OR cookie!
- Log! OR plog!
- Anonym! OR pseudonymous OR unauth!

23. **Steve Hamilton.** Mr. Hamilton is a UXR leading efforts focused on Incognito, including efforts focused on “what we know about Incognito users, what they use it for, and some of the risks we’ve identified.” GOOG-BRWN-00406075. That research is relevant in terms of class member identification, liability, and damages, with Mr. Hamilton noting “Incognito mode is used by [REDACTED] of Chrome users” and that “[u]sers overestimate the protections that Incognito provides.” GOOG-BRWN-00406075-76. Mr. Hamilton identified as one of the “Core Team Members” for Sin Rastro focused on “Incognito Research.” GOOG-BRWN-00148736. His name appears on the first page of an internal Google presentation titled “User Needs & Misconceptions Incognito Mode (IM) Across Google.” GOOG-BRWN-00165706. Another email references an “Incognito Misconceptions survey report” from Mr. Hamilton noting “significant confusion” tied to Incognito. GOOG-BRWN-00392406. Mr. Hamilton should be included as a custodian.

Plaintiffs propose the following searches for Mr. Hamilton:

- Incognito
- inPrivate
- Private! /3 (brows! OR mode)
- OTR OR (off /3 record)
- [REDACTED] OR [REDACTED]
- [REDACTED] OR [REDACTED] OR [REDACTED] or [REDACTED] OR [REDACTED]

24. **Tim Hsieh.** Mr. Hsieh is a Senior Software Engineer at Google who worked on DoubleClick Ad Exchange and Cookie Matcher. Mr. Hsieh helped DoubleClick Ad Exchange connect publishers and advertisers together. [REDACTED] designed, implemented, and launched [REDACTED]



CONTAINS INFORMATION FROM DOCUMENTS
PRODUCED BY GOOGLE AND DESIGNATED BY
GOOGLE AS PROTECTED INFORMATION

Google Counsel
July 16, 2021
Page 18

frameworks to ensure Cookie Matcher complies with various privacy regulations (*e.g.*, GDPR, CCPA, LGPD, and so on). Mr. Hsieh directed Google's efforts to comply with the CCPA and created policy regarding cookies in post-CCPA California. GOOG-BRWN-00245397; GOOG-BRWN-00245558. Mr. Hsieh likely has relevant documents concerning Google's compliance with privacy regulations, which would include compliance regarding the interception and data collection at issue in this case.

Plaintiffs propose the following searches for Mr. Hsieh:

- Incognito
- inPrivate
- Private! /3 (brows! OR mode)
- OTR OR (off /3 record)
- Cookie! OR DoubleClick
- CCPA OR (privacy /5 (law! OR regulation!))

25. **Vivek Sekhar.** Mr. Sekhar appears to be the lead Product Manager for Google's [REDACTED] project. GOOG-BRWN-00178147. Google characterizes this project as its [REDACTED] starting "by the end of 2020," GOOG-BRWN-00221769. Mr. Sekhar likely has highly relevant and unique documents concerning Google's [REDACTED] project.

Plaintiffs propose the following searches for Mr. Sekhar:

- Incognito
- inPrivate
- Private! /3 (brows! OR mode)
- (third OR 3rd OR 3d) /3 cookie!
- [REDACTED] OR [REDACTED]
- [REDACTED] OR [REDACTED] OR [REDACTED] or [REDACTED] OR [REDACTED]

II. Previously Proposed Custodians

In the interest of compromise, Plaintiffs are willing to drop Jian Qiao as a custodian, provided that Google agree to add the following individuals we previously proposed. We have included additional information and ask that Google reconsider its position.

1. **Benj Azose.** Mr. Azose has worked at Google since 2008, and he currently manages the Product Analyst team for Google Chrome that (according to his LinkedIn profile) is [REDACTED]



CONTAINS INFORMATION FROM DOCUMENTS
PRODUCED BY GOOGLE AND DESIGNATED BY
GOOGLE AS PROTECTED INFORMATION

Google Counsel
July 16, 2021
Page 19

“[f]ocused on understanding Chrome users, improving Chrome’s launch process, defining Chrome’s guiding metrics and reporting on changes in key performance indicators inside and outside of Chrome.” Documents produced by Google show that Mr. Azose has been involved with relevant counting metrics tied to Chrome, with its “Omaha” reporting system and where Chrome (at least for a time) [REDACTED]

[REDACTED] GOOG-BRWN-00168232. In July 2020, after this lawsuit was filed, there was a discussion involving Mr. Azose about “moving this data to UMA and removing it from Omaha.” *Id.* Mr. Azose identified himself as “the analyst decision maker on this.” *Id.* The exchange further discusses “Chrome sending stable IDs to Google domains” that “might allow Google to tie browsing sessions together – without any other technologies such as cookies or users signing in.” *Id.* These are all key issues tied to our ongoing disputes. Mr. Azose also likely has records focused on Incognito metrics. For example, in January 2020, he sent an email containing a report on “Clank users” with a “graph” showing users who “use incognito heavily.” GOOG-BRWN-00233853. In December 2019, he was told that Chrome was “not allowed to launch anything that negatively impacts revenue” and asked for help develop “proxies for revenue” and identifying Incognito as one of the “gaps” in the “ability to measure revenue impact.” GOOG-BRWN-00169228-29. Ms. Azose’s name also appears on the first page of a “chrome staples” presentation containing “Device Actives (Omaha)” and “[REDACTED]” noting a process to “log Omnibox in Incognito.” GOOG-BRWN-00048504; GOOG-BRWN-00048512; GOOG-BRWN-00048517. Mr. Azose also appears to have been involved with discussions regarding “changes in feature use” by Chrome users, including with “Incognito” (GOOG-BRWN-00233473), how websites can “detect being in Incognito” (GOOG-BRWN-00169103; *see also* GOOG-BRWN-00182136), certain Incognito “histograms” (GOOG-BRWN-00233108), how “the X-Client-Data header is currently not sent in Chrome” when the “user is in incognito mode” (GOOG-BRWN-00233093), and how [REDACTED] with other “incognito usage stats” (GOOG-BRWN-00233072). In connection with [REDACTED], Mr. Azose was also asked for “data to measure/estimate incognito traffic in Chrome” (GOOG-BRWN-00233078). Mr. Azose’s key role in evaluating those metrics and revenue impacts, including with Incognito, establish a basis to include him as a custodian.

Plaintiffs propose the following searches for Mr. Azose:

- Incognito
- inPrivate
- Private! /3 (brows! OR mode)
- Omaha OR UMA
- “Identifier! OR UID
- “opt out” OR “opt-out”
- [REDACTED] or [REDACTED]
- (tie OR tying OR link!) /5 (brows! OR session!)



CONTAINS INFORMATION FROM DOCUMENTS
PRODUCED BY GOOGLE AND DESIGNATED BY
GOOGLE AS PROTECTED INFORMATION

Google Counsel
July 16, 2021
Page 20

- [REDACTED] OR [REDACTED] OR [REDACTED] or [REDACTED] OR [REDACTED]

2. **Nina Ilieva.** As mentioned in our May 21 letter, Ms. Ilieva has been involved with developing Google infrastructures to manage user identity in the ads space, which is relevant to the issue of how Google tracks users' private browsing. For example, according to internal Google documents, Google asked employees to "update our public facing documents that discuss cookies" as "part of our consent improvements for signed out users." GOOG-BRWN-00176119. Ms. Ilieva seems to have been involved with this Google project, which aims to improve "key things," including "help[ing] users understand abstract construct of 'cookies' and how they work." GOOG-BRWN-00176120. She noted that the Ads team was "doing a reclassification of their cookies." GOOG-BRWN-00176119. Google initially refused to make her a custodian (in part) because Ms. Ilieva reported to Greg Fair, a current custodian in this case. *See* Google's May 19 letter. But Google recently clarified that Ms. Ilieva "no longer reports to Mr. Fair." *See* Google's June 21 Letter. Ms. Ilieva likely possesses unique documents concerning user consent in the context of signed out users and should be made a custodian.

Plaintiffs propose the following searches for Ms. Ilieva:

- Incognito
- inPrivate
- Private! /3 (brows! OR mode)
- OTR OR (off /3 record)
- Consent!
- Cookie!

3. **Sammit Adhya.** Mr. Adhya appears to have unique knowledge about Google's efforts and users' privacy expectations when it comes to Incognito mode. For example, following "user studies on unauth [sic] transparency/controls," he explained that "part of the challenge we face with both Android and Chrome is the definition of incognito." GOOG-BRWN-00222150. He noted that it "seems clear that users don't have a good sense of identity management," that "[e]ven the most basic questions around sign-in/sign-out state are completely misunderstood," and that "[u]sers have no idea . . . what is happening in their current state in terms of data collection." *Id.* He also asked if Google was "willing to trade data/revenue for user trust and brand reputation," and "[h]ow we want to define incognito/private browsing," including whether Incognito mode is "purely for local privacy" or for "privacy from Google." *Id.* In another internal discussion, Mr. Adhya explained how Google wanted to convey the message to users that if they "want to prevent Google from collecting data," they should be "one step away from that in *any* of our products by using Incognito." GOOG-BRWN-00177525. Mr. Adhya also espoused strong beliefs that Google should simplify, not complicate, its privacy controls, stating users should not require a "cognitive load" to understand and operate those controls. *Id.* Mr. Adhya also acknowledged that there are misconceptions with Incognito and Google should clarify [REDACTED] Google. And



CONTAINS INFORMATION FROM DOCUMENTS
PRODUCED BY GOOGLE AND DESIGNATED BY
GOOGLE AS PROTECTED INFORMATION

Google Counsel
July 16, 2021
Page 21

in a different internal discussion, Mr. Adhya noted a “search detecting Incognito” issue and remarked, “yikes, doubled down on a promise we don[’t] keep.” GOOG-BRWN-00176480. Mr. Adhya was also involved with discussions about whether Incognito activity is saved in a user’s Google Account. GOOG-BRWN-00212393. Although Mr. Adhya is not a member of Google’s [REDACTED] group/project, he was often encouraged to contact [REDACTED] team members to better understand the project and coordinate. GOOG-BRWN-00177701, GOOG-BRWN-00178147. Further, Mr. Adhya was involved in [REDACTED] and third-party cookie blocking discussions with other internal Google groups. GOOG-BRWN-00177626, GOOG-BRWN-00177764, GOOG-BRWN-00182715.

Plaintiffs propose the following searches for Mr. Adhya:

- Incognito!
- inPrivate
- Private! /3 (brows! OR mode)
- User! /15 (study OR studies OR understand! OR confuse!)
- “Identity management”
- “Sin Rastro” AND (fail* OR review* OR analy*)
- [REDACTED] OR [REDACTED] OR [REDACTED]
- (third OR 3rd OR 3d) /3 cookie*
- Zw* OR Biscotti OR pseudo*
- ePrivacy
- consent* /3 ready
- “summer moment”
- account /3 particle
- [REDACTED] OR [REDACTED] OR [REDACTED] or [REDACTED] OR [REDACTED]

4. **Suneeti Shah Vakharia.** Ms. Vakharia appears to have knowledge about important issues of user consent. She has been involved in developing “plans to improve our signed out user consent” and projects involving Incognito mode like Sin Rastro. GOOG-BRWN-00176804. She has also been tasked with “[p]roviding new users with critical privacy choices during account creation to understand and control the information they share with Google when signed in or when signed out.” GOOG-BRWN-00204666. Ms. Vakharia likely has documents relevant to user consent, an important issue in this case.

Plaintiffs propose the following searches for Ms. Vakharia:

- Incognito!
- inPrivate
- Private! /3 (brows! OR mode) [REDACTED] [REDACTED]



CONTAINS INFORMATION FROM DOCUMENTS
PRODUCED BY GOOGLE AND DESIGNATED BY
GOOGLE AS PROTECTED INFORMATION

Google Counsel
July 16, 2021
Page 22

- OTR OR (off /3 record)
- “Sin Rastro”
- User! /15 (understand! OR confuse!)
- Consent!

5. **Richard Jui-Chieh Hsu.**⁹ Mr. Hsu appears as the main engineer in Google’s [REDACTED] a [REDACTED] related project. GOOG-BRWN-001521201. That project [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] GOOG-BRWN-00152203. Given his engineering role in this Incognito-related project, Mr. Hsu likely has unique and highly relevant documents.

Plaintiffs propose the following searches for Mr. Hsu:

- Incognito!
- inPrivate
- Private! /3 (brows! OR mode)
- OTR OR (off /3 record)
- Zw! OR biscotti OR cookie!
- [REDACTED]

III. PWG Custodians

Aside from the three individuals Google identified, see Google’s June 25 email, we still have not received information about who is part of Google’s Privacy Working Group, including without limitation the Chrome PWG. Please provide that as soon as possible.

IV. Google-Selected and Agreed-To Custodians

Based on our review of Google’s June 18 production, it has become apparent that there are some additional searches needed to identify relevant documents that should be produced. Plaintiffs propose that Google run the following additional searches for the ten Google-Selected

⁹ It’s not clear if “Richard Hsu” (identified in Mr. Bernston’s deposition, see Bernston Tr. at 260:1–260:24) and “Richard Jui-Chieh Hsu” are the same person, based on Google’s June 21 letter, which refused to add Mr. Hsu as a custodian but did not mention whether he is or is not currently employed by Google. Please clarify. [REDACTED]



CONTAINS INFORMATION FROM DOCUMENTS
PRODUCED BY GOOGLE AND DESIGNATED BY
GOOGLE AS PROTECTED INFORMATION

Google Counsel
July 16, 2021
Page 23

Custodians—Glenn Bernston, Deepti Bhatnagar, Sabine Borsay, Greg Fair, Helen Harris, Abdelkarim Mardini, Justin Schuh, Dan Stone, Alexei Svitkine, and Keith Wright, and also to the four agreed-to custodians—Adrienne Porter Felt, Sam Heft-Luthy, Russ Ketchum, and Chris Liao.¹⁰

No.	Search Term	Basis for Adding
1	Eprivacy OR (consent! /3 ready) OR consentless	This search is likely to hit on relevant documents concerning Google's efforts to "move to a consentless ready incognito." GOOG-BRWN-00176943.
2	(summer OR privacy) /2 moment	Google's Summer Privacy Moment was "comprised of privacy and security product announcements," which "[l]anded neutral to positive press coverage across major outlets globally." GOOG-BRWN-00154766. One of Summer Privacy Moment's objectives was to "[s]trengthen Google's position as an industry leader when it comes to data privacy," and included messages on how Google "keep[s] your information private" by providing "[e]asier access to Incognito mode." GOOG-BRWN-00154767; GOOG-BRWN-00154768.
3	██████████ OR ██████████	This search is likely to hit on relevant documents concerning Google's "third party cookie blocking feature in Incognito mode." GOOG-BRWN-00042435.
4	GWS /10 (ID OR identif!)	This search is likely to hit on relevant documents relating to Google's GWS ID, which is used to identify Incognito browsing. GOOG-BRWN-00168636.

¹⁰ Regarding the four agreed-to custodians, the parties are still negotiating their searches. Plaintiffs proposed that Google apply to Ms. Porter Felt, Mr. Heft-Luthy, and Mr. Ketchum the same searches Google applied to the Google-selected custodians, see Plaintiffs' June 22 letter, and for Mr. Liao, Plaintiffs proposed that Google apply a smaller set of searches, see Plaintiffs' July 2 email. The searches identified in this letter are in addition to those proposed searches. Lastly, as a point of clarification, Plaintiffs' June 22 Letter mistakenly referred to the "Court-ordered" custodians, instead of the "Google-selected" custodians, when referring to the searches that Google should apply to Mr. Ketchum.

██████████ ██████████



CONTAINS INFORMATION FROM DOCUMENTS
PRODUCED BY GOOGLE AND DESIGNATED BY
GOOGLE AS PROTECTED INFORMATION

Google Counsel
July 16, 2021
Page 24

ad5	OTR OR (off /3 record)	This search is likely to hit on relevant documents describing Incognito mode. GOOG-BRWN-00193106.
6	████████ OR ██████ OR ██████	This search is likely to hit on relevant documents regarding Google's efforts to gain "user trust and choice." GOOG-BRWN-00150516. ; <i>see also</i> GOOG-BRWN-00205911; GOOG-BRWN-00205913 ("████████" is focused on how "[u]sers should be and feel in control" and how Google should "[b]e transparent about user data collection, storage, and uses" and "[m]ake user choices meaningful and understandable.").
7	GaiaMint OR "Gia Mint"	This search is likely to hit on relevant documents concerning "GaiaMint," a "service that translates credentials into short lived, signed tokens (known as 'mints' or "GaiaMints." GOOG-BRWN-00057046. A GaiaMint is an example of an "authenticator." <i>Id.</i>
8	Zw! OR biscotti OR cookie!	This search is likely to hit on relevant documents concerning Google's use of twice-baked and other relevant cookies.
9	UMA OR "User Metric Analytics"	This search is likely to hit on relevant documents concerning Google's "User Metrics Analytics," which appears to be a back end process for Chrome that logs and syncs Google Chrome usage data.
10	Finch	This search is likely to hit on relevant documents concerning Finch, a "Chrome experiments framework" which is used to "facilitate" the understanding of "the impact of Chrome experiments on user behavior on Google properties." GOOG-BRWN-00051406. Finch is relevant to identifying potential class members.
11	██████	This search is likely to hit on relevant documents concerning "████████," "████████" ████████████████████ ████████████████████ ████████████████████ ████████." GOOG-BRWN-00061091.
12	██████	This search is likely to hit on relevant documents concerning ██████, "████████████████████"



CONTAINS INFORMATION FROM DOCUMENTS
PRODUCED BY GOOGLE AND DESIGNATED BY
GOOGLE AS PROTECTED INFORMATION

Google Counsel
July 16, 2021
Page 25

		[REDACTED] [REDACTED].” GOOG-BRWN-00209131.
13	[REDACTED]	This search is likely to hit on relevant documents concerning “[REDACTED],” which is a [REDACTED],” GOOG-BRWN-00061594, and “[REDACTED],” which is the [REDACTED] GOOG-BRWN-00061915.
14	[REDACTED]	This search is likely to hit on relevant documents concerning Google’s goal to “[s]ystemically improve user privacy protection.” GOOG-BRWN-00150515.
15	X-Client /10 (data OR header OR variation)	This search is relevant in terms of the parties’ ongoing dispute regarding identification of class members, with Google employees admitting that this information can be used to identify Incognito browsing.
16	[REDACTED]	“[REDACTED]” appears to be the codename for a [REDACTED]. <i>See, e.g.,</i> GOOG-BRWN-00152234.

V. Court-Ordered Custodians

Plaintiffs propose that Google apply the following additional searches to six of the seven Court-ordered custodians—Unni Narayanan, Jan Hannemann, Eric Miraglia, Rahul Roy-Chowdhury, Stephan Micklitz, and Brian Rakowski.

No.	Search Term	Basis for Adding
1	[REDACTED] OR [REDACTED] OR [REDACTED] OR [REDACTED] OR [REDACTED] OR [REDACTED] OR [REDACTED] OR [REDACTED] [REDACTED] OR [REDACTED] OR [REDACTED]	As explained above, these appear to be relevant Google codenames, which these custodians may have used.
2	Zw! OR biscotti OR unauth!	This search is necessary to ensure that we capture documents concerning the private browsing data at issue in this case, which Google associates with these identifiers and refers to as unauthenticated or unauth.

BSF

CONTAINS INFORMATION FROM DOCUMENTS
PRODUCED BY GOOGLE AND DESIGNATED BY
GOOGLE AS PROTECTED INFORMATION

Google Counsel
July 16, 2021
Page 26

Sincerely,

A handwritten signature in blue ink, appearing to read "Beko Reblitz-Richardson", with a long horizontal flourish extending to the right.

Beko Reblitz-Richardson

[REDACTED]

EXHIBIT 35
Redacted Version of
Document Sought to
be Sealed

quinn emanuel trial lawyers | washington, dc

1300 I Street NW, Suite 900, Washington, District of Columbia 20005-3314 | TEL (202) 538-8000 FAX (202) 538-8100

WRITER'S EMAIL ADDRESS
josefansorge@quinnemanuel.com

HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY

October 1, 2021

VIA E-MAIL

Special Master Douglas Brush
(douglas.brush@accelconsulting.llc)
Accel Consulting, LLC

Timothy Schmidt
Accel Consulting, LLC

David A. Straite (dstraite@dicellolevitt.com)
Dicello Levitt Gutzler

Lesley Weaver (lweaver@bfalaw.com)
Bleichmar Fonti & Auld LLP

Jay Barnes (jaybarnes@simmonsfirm.com)
Simmons Hanly Conroy LLC

Re: Google's Submission in Response to Special Master's Request for Technical
Descriptions of Burdens Associated With Providing Requested Information
Calhoun v. Google LLC, 20-cv-05416-LHK (SVK) (N. D. Cal.)

Dear Special Master Brush:

We write in response to your September 30, 2021 request for a technical description of the burdens associated with providing the additional information Plaintiffs have requested. Since Plaintiffs in both cases have already made selections under Step 3, we believe that the technical burdens associated with providing additional information under Steps 1 and 2 are neither proportional, nor required, nor beneficial, to efficiently resolving the disputes currently before the Special Master. *See* Order Following September 30, 2021 Discovery Hearing, Dkt. 329 ("Simply put, each and every transmission, whether or not authorized, neither can nor should be the subject of discovery in this case. Litigation of the size and magnitude of this action requires selection of discovery targets which allow the Parties the opportunity to prove their claims or defenses to a trier of fact within the bounds of Federal Rule of Civil Procedure 26.")

Please do not hesitate to let us know if you would benefit from any additional information or explanatory materials regarding the issues described below.

quinn emanuel urquhart & sullivan, llp

ATLANTA | AUSTIN | BOSTON | BRUSSELS | CHICAGO | HAMBURG | HONG KONG | HOUSTON | LONDON | LOS ANGELES | MANNHEIM | MIAMI |
MUNICH | NEUILLY-LA DEFENSE | NEW YORK | PARIS | PERTH | SALT LAKE CITY | SAN FRANCISCO | SEATTLE | SHANGHAI | SILICON VALLEY |
STUTTGART | SYDNEY | TOKYO | WASHINGTON, DC | ZURICH

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY**Step 1: Burden of Identifying Every Data Source Potentially Containing Responsive ESI**

- Google maintains numerous distinct systems holding “data sources” which could potentially contain responsive ESI. These range from structured key-value storage systems (e.g. BigTable and [REDACTED]) to log systems storing data sequentially ([REDACTED]). No single tool exists to query all of these distinct systems and generate a list of all data sources that may contain the specific data at issue in this case. The systems are designed independently for product usage. There is also no single team responsible for all potentially relevant data sources. To compile the requested information, separate subject matter experts for each system were required to identify, analyze, and describe potentially relevant data sources.
- Because individual product teams are responsible for data associated with their products, subject to Google’s policies, experts from different product teams were also required to identify potentially relevant sources.
- Even within a product, Google has many different systems that record log entries for different purposes, ranging from simple debugging to providing enterprise-level reporting to its customers. Teams are functionally differentiated and engineers in any given team will have responsibilities for different tools.
- Some of Google’s log processing systems producing reports for publishers entail configurations (written in [Borg Configuration Language](#)) that list multiple logs. However, these configurations only cover logs processed by that specific pipeline. Listing all potentially relevant logs, even within display ads, requires identifying, contacting, and working with several different teams and experts.

Step 2: Burden of Compiling Field Names

- Google stores its logs records in [protocol buffers](#). Protocol buffers related to the selected log sources are complex and include nested sub-messages that consist of other protocol buffers, that contain further nested sub-messages, and so forth. Each message file contains information about the name, type, identifying field number, and (in some cases) a comment about the field. To save space on disk, a protocol buffer record is encoded in a format in which the fields are identified by tag numbers.
- Because the logs in question have fields and message files from multiple protocol buffer files, Google cannot produce a single “.proto” file, but rather would be required to compile a list of hundreds of files—a complex exercise that will require many software engineering hours. Similar to how C++ compilers can walk through #include statements to produce a binary with all the relevant code and libraries linked in—but there are no readily available tools to reconstruct all the relevant source code that went into that specific binary—proto files import other proto files, using subsections of those files. Moreover, proto files related to the selected data sources are source code: they are submitted as source code, reviewed as source code, and run as source code.

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY

- A protocol buffer contains all *possible* tags that could contain data. With very few exceptions—such as the limited number fields that have the rarely used “required” tag—there is no requirement for any given field to be filled in. Moreover, it is impossible to enforce the semantics of what a field is used for from product to product, or even record to record. Some protocol buffers, such as those used in ad query logs or frontend logs, are shared across multiple Google products and the vast majority of fields listed therein will contain no data in a given record. For example, many fields pertain only to ads shown on Google’s search page and are irrelevant to ads on third-party websites.
- Providing a list of fields in a proto that are actually filled/used for the data at issue, is also burdensome. Google has no existing tool that provides a listing of populated fields based on a given set of conditions. In theory, Google engineers could create a Flume pipeline to parse each individual record, filter-in matching product/criteria, enumerate the filled fields, and add those to a running set. However, this is a non-trivial program to write, test, submit, and validate. Running this program over more than a handful of recent days would also require significant computer resources, as the potentially relevant log sources are in the hundreds of petabyte range. This list of fields would also contain highly sensitive information related to Google’s ads serving infrastructure and abuse detection, that is irrelevant to this matter and whose disclosure could cause Google substantial economic harm.

Step 2: Burden of Field Descriptions

- The semantics and usage of fields, even in a single data source, change over time, but given the difficulty in updating all references to a given field, names are very rarely changed. Because each product or record may use the same field in a different way, there is no single fixed definition that can be applied to all fields. To ensure that field descriptions are accurate, up to date, and fully capture the current field semantics, each description has to be verified by a team of engineers.
- No readily available tool exists to look up existing comments for a list of fields to create a “dictionary” of field names and comments. To generate the descriptions provided to date under Step 2, Google engineers had to hand copy, review, and verify field descriptions. This laborious process does not scale and is infeasible for multiple sources with thousands of fields.
- There is no single subject matter expert at Google that can, or could, provide descriptions for all data sources, let alone all fields within any given data source. Different subject matter experts are required to provide clear, precise description of fields (or group of fields) in any given context. For many fields, the subject matter expert has to consult additional source code and documentation to understand the logic whereby the field is written or read. On average, it should take a fast, knowledgeable engineer at least five minutes to write and verify a specific field description for a field they understand and use regularly. For

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY

100 fields, that equates to a full day of work, just for relatively simple fields. Performing code archeology to determine possible changes to these fields or updates to semantics would further greatly increase the effort required. The field descriptions provided so far were generated manually by engineers working long hours, in addition to their usual responsibilities.

Step 3: Running searches on Selected Data Sources

- Google’s logging systems are not designed to facilitate Googlers searching for, or accessing, data for specific individual users. To the contrary, Google’s systems are purposely designed to prevent employees from querying data for specific users. These protections entail additional levels of access-control lists (“ACLs”) on specific fields in logs, including all user identifiers. For any one Googler to be able to access fields that contain raw user identifiers, they must obtain special permissions, and receive approvals from privacy review committees. This process is purposely designed to limit access to sensitive information and it is enforced through a number of technical barriers.
- In addition to the ACLs, publisher configurations, Google policies, and/or legislation require further encryption of identifiers. Many are specifically labelled as DO_NOT_ACCESS_WITHOUT_A_PRIVACY_REVIEW; these fields require privacy reviews and specialized keys (controlled by the privacy reviewers) to gain access. These systems were designed to only allow very specialized code to access. To perform the requested searches at short notice, multiple engineers need to gain permissions, and write this code.
- For debugging purposes, Google maintains 8 days of various logs sources in an optimized format that is queryable by Dremel. (Dremel is a distributed system for quickly querying large datasets. Users write SQL queries that are then executed by Dremel’s execution engine over data stored in a special columnar data format.) Beyond 8 days, the data is stored in a less optimized format to save disc space allowing the logs to be preserved for longer. To query beyond 8 days, Google must use more specialized tooling, such as Flume pipelines, and write custom SQL pipelines that search and process data. (Flume is a framework for executing batch (as opposed to streaming) workloads in parallel over large datasets. Engineers write Flume pipelines in C++ or Java and run these pipelines on Borg to process data. Unlike Dremel, Flume does not require data to be stored in a Columnar format, but it does require significantly more developer time to configure, launch, and tune than a simple Dremel query.) Creating a new search in Flume requires writing C++ scripts and BORG configurations that have to be vetted and submitted for code review.
- Searching across historic log files entails significant computing resources. For example, [REDACTED]

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY

We hope this information is helpful and look forward to continuing to work with Plaintiffs and the Special Master to collaboratively resolve the disputes currently before the Special Master.

Respectfully,

QUINN EMANUEL URQUHART & SULLIVAN, LLP

A handwritten signature in black ink, appearing to read "Josef Ansorge". The signature is written in a cursive, flowing style.

Josef Ansorge

JA

EXHIBIT 36
Redacted Version of
Document Sought to
be Sealed



November 9, 2021

SENT VIA EMAIL

QUINN EMANUEL URQUHART & SULLIVAN, LLP

Diane M. Doolittle
(dianedoolittle@quinnemanuel.com)
Thao Thai (thaothai@quinnemanuel.com)
555 Twin Dolphin Drive, 5th Floor
Redwood Shores, CA 94065

Andrew H. Schapiro
(andrewschapiro@quinnemanuel.com)
191 N. Wacker Drive, Suite 2700
Chicago, IL 60606

Stephen A. Broome
(stephenbroome@quinnemanuel.com)
Viola Trebicka
(violatrebicka@quinnemanuel.com)
865 S. Figueroa Street, 10th Floor
Los Angeles, CA 90017

William A. Burck
(williamburck@quinnemanuel.com)
Josef Ansorge
(josefansorge@quinnemanuel.com)
1300 I Street, N.W., Suite 900
Washington, D.C. 20005

Jonathan Tse
(jonathantse@quinnemanuel.com)
50 California Street, 22nd Floor
San Francisco, CA 94111

Jomaire Crawford
(jomairecrawford@quinnemanuel.com)
51 Madison Avenue, 23rd Floor
New York, NY 10010

**Re: *Chasom Brown, et al., v. Google LLC*, Case No. 5:20-cv-03664-LHK
Chris Liao Document Issues**

Dear Counsel,

As the parties have agreed, Plaintiffs will be deposing Chris Liao on December 2 and 3. In connection with that deposition, we have identified certain issues with Google's document productions. In addition to producing earlier-in-time emails, Plaintiffs ask that you please quickly investigate the issues below and produce any additional documents no later than November 23.

For the following documents, please identify (and if they have not already been produced, please produce and identify) the following links:

- GOOG-CABR-03664145: "3M New UUIDs/section"; http://shortn_Bfff6ggAisk"; "[some useful queries](#)"; "[example](#)"; "Implementation and Rollout Plan: [\[b/121144670\]](#)" "[\[b/159213961\]](#)"; "[\[b/161366859\]](#)".

BOIES SCHILLER FLEXNER LLP



Google Counsel
October 25, 2021
Page 2

- GOOG-CABR-03664108: “see go/zwieback/resident-properties.md for a full treatment”; “for a full inventory see this file”; [b/133456674]”.
- GOOG-CABR-03665840: [REDACTED]
- GOOG-CABR-04706890: “Go/id-filtering”, “go/id-joinability”, “go/id-logging”.
- GOOG-CABR-03664108: “for a full inventory see this file”; “such as described here”, “the standard production build-horizon of 6 months”, and “informational co-diversion in GWS”.
- GOOG-CABR-03665840: “go/display-[REDACTED]”, “go/display-[REDACTED]”, “go/display-[REDACTED]”, “go/display-[REDACTED]”, “go/display-[REDACTED]”, “go/display-[REDACTED]”, “go/display-[REDACTED]”, “//contentads/identity/[REDACTED]”, “go/pic-gmob-slides”, “go/[REDACTED]”.
- GOOG-CABR-00393660: “go/unified-display-signed-in”
- GOOG-CABR-04205200: “go/[REDACTED]”.
- GOOG-CABR-00547295: “log-based monitoring”, “monitoring and impact analysis”, “here”, “inferred”, “different levels of accuracy”, “input signals”, “go/chromeguard-monitor”, “no significant changes in incognito usage”, “(proxy) metrics” for “Search” and “Display”.

From GOOG-CABR-04706890, identified above, please also identify the citations referenced in footnote four.

GOOG-CABR-04695992 includes images and graphs that are illegible in the version produced. Please produce a version in which they are legible, or produce the version of the images and graphs that appear in this document in legible form.

Please respond to this letter by November 16.

Sincerely,

A handwritten signature in black ink, appearing to read "Erika Nyborg-Burch", is placed above the typed name.

Erika Nyborg-Burch

EXHIBIT 37

Geoffrey Grundy

From: Sara Jenkins
Sent: Tuesday, January 11, 2022 10:26 PM
To: 'Erika Nyborg-Burch'; QE Brown
Cc: googleteam@lists.susmangodfrey.com; Lesley Weaver; Angelica M. Ornelas (aornelas@bfalaw.com); Julie Law; An V. Truong (atruong@simmonsfirm.com); Jay Barnes; David Straite; Adam Prom; scruz@dicellolevitt.com
Subject: RE: Brown v. Google LLC (N.D. Cal. Case No. 20-cv-03664)- request for Brown depositions (Bert Leung, Michael Kleber, Hyewon Jun, and Deepti Bhatnagar)

Counsel,
Bert Leung is available for deposition on February 25. Hyewon Jun is available for deposition on February 11.

Regards,
Sara

From: Erika Nyborg-Burch [mailto:enyborg-burch@bsfillp.com]
Sent: Monday, January 10, 2022 7:34 AM
To: Sara Jenkins <sarajenkins@quinnemanuel.com>; QE Brown <qebrown@quinnemanuel.com>
Cc: googleteam@lists.susmangodfrey.com; Lesley Weaver <lweaver@bfalaw.com>; Angelica M. Ornelas (aornelas@bfalaw.com) <aornelas@bfalaw.com>; Julie Law <jlaw@bfalaw.com>; An V. Truong (atruong@simmonsfirm.com) <atruong@simmonsfirm.com>; Jay Barnes <jaybarnes@simmonsfirm.com>; David Straite <dstraite@dicellolevitt.com>; Adam Prom <aprom@dicellolevitt.com>; scruz@dicellolevitt.com
Subject: RE: Brown v. Google LLC (N.D. Cal. Case No. 20-cv-03664)- request for Brown depositions (Bert Leung, Michael Kleber, Hyewon Jun, and Deepti Bhatnagar)

[EXTERNAL EMAIL from enyborg-burch@bsfillp.com]

Sara,

Have you identified dates that Mr. Leung will be available for a deposition? Can you also please let us know what alternative dates Hyewon Yun is available?

Thanks,
Erika

From: Erika Nyborg-Burch
Sent: Thursday, December 30, 2021 7:31 AM
To: Sara Jenkins <sarajenkins@quinnemanuel.com>; QE Brown <qebrown@quinnemanuel.com>
Cc: googleteam@lists.susmangodfrey.com; Lesley Weaver <lweaver@bfalaw.com>; Angelica M. Ornelas (aornelas@bfalaw.com) <aornelas@bfalaw.com>; Julie Law <jlaw@bfalaw.com>; An V. Truong (atruong@simmonsfirm.com) <atruong@simmonsfirm.com>; Jay Barnes <jaybarnes@simmonsfirm.com>; David Straite <dstraite@dicellolevitt.com>; Adam Prom <aprom@dicellolevitt.com>; scruz@dicellolevitt.com
Subject: RE: Brown v. Google LLC (N.D. Cal. Case No. 20-cv-03664)- request for Brown depositions (Bert Leung, Michael Kleber, Hyewon Jun, and Deepti Bhatnagar)

Thank you, Sara.

We are confirming January 14 for Michael Kleber and January 21 for Deepti Bhatnagar.

For Hyewon Yun, we request that you propose some additional dates that this deponent is available.

We will wait to hear back as to Mr. Leung's availability when he returns next week.

Best,
Erika

From: Sara Jenkins <sarajenkins@quinnemanuel.com>
Sent: Tuesday, December 28, 2021 5:53 PM
To: Erika Nyborg-Burch <enyborg-burch@bsfillp.com>; QE Brown <gebrown@quinnemanuel.com>
Cc: googleteam@lists.susmangodfrey.com; Lesley Weaver <lweaver@bfalaw.com>; Angelica M. Ornelas <aornelas@bfalaw.com> <aornelas@bfalaw.com>; Julie Law <jlaw@bfalaw.com>; An V. Truong <atruong@simmonsfirm.com> <atruong@simmonsfirm.com>; Jay Barnes <jaybarnes@simmonsfirm.com>; David Straite <dstraite@dicellolevitt.com>; Adam Prom <aprom@dicellolevitt.com>; scruz@dicellolevitt.com
Subject: RE: Brown v. Google LLC (N.D. Cal. Case No. 20-cv-03664)- request for Brown depositions (Bert Leung, Michael Kleber, Hyewon Jun, and Deepti Bhatnagar)

Counsel,
Please see the proposed dates below.

Michael Kleber - January 14
Hyewon Jun – January 20
Deepti Bhatnagar – January 21

Mr. Leung is out of the office and will not be returning until January 4. We will provide you with his availability as soon as we can.

Regards,
Sara

From: Erika Nyborg-Burch [<mailto:enyborg-burch@bsfillp.com>]
Sent: Tuesday, December 21, 2021 4:04 PM
To: QE Brown <gebrown@quinnemanuel.com>
Cc: googleteam@lists.susmangodfrey.com; Lesley Weaver <lweaver@bfalaw.com>; Angelica M. Ornelas <aornelas@bfalaw.com> <aornelas@bfalaw.com>; Julie Law <jlaw@bfalaw.com>; An V. Truong <atruong@simmonsfirm.com> <atruong@simmonsfirm.com>; Jay Barnes <jaybarnes@simmonsfirm.com>; David Straite <dstraite@dicellolevitt.com>; Adam Prom <aprom@dicellolevitt.com>; scruz@dicellolevitt.com
Subject: Brown v. Google LLC (N.D. Cal. Case No. 20-cv-03664)- request for Brown depositions (Bert Leung, Michael Kleber, Hyewon Jun, and Deepti Bhatnagar)

[EXTERNAL EMAIL from enyborg-burch@bsfillp.com]

Counsel,

Brown Plaintiffs request deposition dates for Bert Leung, Michael Kleber, Hyewon Jun, and Deepti Bhatnagar. Thank you.

Best,

Erika Nyborg-Burch

Associate

BOIES SCHILLER FLEXNER LLP

44 Montgomery Street, 41st Floor

San Francisco, CA 94104

(t) 415 293 6806

enyborg-burch@bsfllp.com

www.bsfllp.com

Admitted to practice in New York only; Not admitted in California

The information contained in this electronic message is confidential information intended only for the use of the named recipient(s) and may contain information that, among other protections, is the subject of attorney-client privilege, attorney work product or exempt from disclosure under applicable law. If the reader of this electronic message is not the named recipient, or the employee or agent responsible to deliver it to the named recipient, you are hereby notified that any dissemination, distribution, copying or other use of this communication is strictly prohibited and no privilege is waived. If you have received this communication in error, please immediately notify the sender by replying to this electronic message and then deleting this electronic message from your computer. [v.1 08201831BSF]

The information contained in this electronic message is confidential information intended only for the use of the named recipient(s) and may contain information that, among other protections, is the subject of attorney-client privilege, attorney work product or exempt from disclosure under applicable law. If the reader of this electronic message is not the named recipient, or the employee or agent responsible to deliver it to the named recipient, you are hereby notified that any dissemination, distribution, copying or other use of this communication is strictly prohibited and no privilege is waived. If you have received this communication in error, please immediately notify the sender by replying to this electronic message and then deleting this electronic message from your computer. [v.1 08201831BSF]

EXHIBIT 38

Geoffrey Grundy

From: Alex Frawley <AFrawley@susmangodfrey.com>
Sent: Sunday, February 13, 2022 3:11 PM
To: Sara Jenkins; QE Brown
Cc: googleteam@lists.susmangodfrey.com
Subject: RE: Leung hit counts

[EXTERNAL EMAIL from afrawley@susmangodfrey.com]

Hi Sara,

Thanks for the call earlier. If Google will review all de-duplicated documents that hit on Plaintiffs' search term and timeframe proposal, then Plaintiffs agree that the Leung deposition scheduled for the 25th can move forward on that day provided that: (1) any documents related to the 2020 Incognito detection analysis are produced by February 18, including the non-custodial documents Google already agreed to produce, in addition to the Leung custodial documents at issue now; (2) seven days before the deposition, Google provides a privilege log for any and all documents withheld from Leung's custodial and non-custodial documents; and (3) Google agree to work with Plaintiffs to expeditiously produce hyperlinked documents that are referenced in the upcoming Leung production, all to be produced or otherwise identified in an updated privilege log prior to the deposition.

Plaintiffs also can confirm that we right now do not anticipate seeking to request that any additional Google employees be added as a custodian. But that can of course change based on our ongoing review of Google's productions, including the ongoing production of documents related to the Incognito detection analysis and the ongoing production of documents previously withheld as privileged.

Best,
 Alex

From: Sara Jenkins <sarajenkins@quinnemanuel.com>
Sent: Sunday, February 13, 2022 12:48 PM
To: Alex Frawley <AFrawley@susmangodfrey.com>
Cc: brichardson <brichardson@bsflp.com>
Subject: RE: Leung hit counts

EXTERNAL Email

We do not yet have de-duplicated hit counts. Below are the hit counts that we have, pre-de-deduplication. I think it makes sense to speak at 11 as I do not know when the de-duplicated counts will be ready. I'm at 650-703-3589 if you want to speak by phone, or please circulate a Zoom link.
 Thanks.

	Documents	Documents w/Family	Unique Documents
Incognito	1510	1731	1138

ChromeGuard	515	600	156
"Chrome Guard"	123	204	17

From: Alex Frawley [<mailto:AFrawley@susmangodfrey.com>]
Sent: Sunday, February 13, 2022 8:45 AM
To: Sara Jenkins <sarajenkins@quinnemanuel.com>
Cc: brichardson <brichardson@bsfllp.com>
Subject: RE: Leung hit counts

[EXTERNAL EMAIL from afrawley@susmangodfrey.com]

Hi Sara,

11 am works for me, so let's plan to chat then (assuming the hit counts are ready). Thanks!

From: Sara Jenkins <sarajenkins@quinnemanuel.com>
Sent: Sunday, February 13, 2022 2:06 AM
To: Alex Frawley <AFrawley@susmangodfrey.com>
Cc: brichardson <brichardson@bsfllp.com>
Subject: Re: Leung hit counts

EXTERNAL Email

Hi Alex,
I hope to have something for you in the morning. If so, I'm free to speak at 11am Pacific if that works for you.

Get [Outlook for Android](#)

From: Alex Frawley <AFrawley@susmangodfrey.com>
Sent: Saturday, February 12, 2022 1:09:25 PM
To: Sara Jenkins <sarajenkins@quinnemanuel.com>
Cc: brichardson <brichardson@bsfllp.com>
Subject: Leung hit counts

[EXTERNAL EMAIL from afrawley@susmangodfrey.com]

Hi Sara,

When can we expect the Leung hit counts? Should we make a plan to chat tomorrow afternoon since we need to update the Court on Monday?

Best,
Alex

Alexander P. Frawley | Susman Godfrey LLP
1301 Avenue of the Americas, 32nd Floor | New York, NY 10019

212.729.2044 (office) | 917.599.6613 (cell)

afrawley@susmangodfrey.com | www.susmangodfrey.com

EXHIBIT 39
Redacted Version of
Document Sought to
be Sealed

---o0o---

CHASOM BROWN, et al.,)
on behalf of themselves and)
all others similarly)
situated,)
)
Plaintiffs,) Case No.
) 5:20-cv-03664-LHK
vs.)
)
GOOGLE LLC,)
)
Defendant.)
_____)

---o0o---

Videotaped Zoom Deposition of
WING PAN "BERT" LEUNG
CONFIDENTIAL
Friday, March 4, 2022

— — — o 0 o — — —

Katy E. Schmidt
RPR, RMR, CRR, CSR 13096
Veritext Job No.: 5091833

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

---o0o---

CHASOM BROWN, et al.,)
on behalf of themselves and)
all others similarly)
situated,)

)
) Case No.
) 5:20-cv-03664-LHK
vs.)

)
GOOGLE LLC,)

)
Defendant.)

_____)

BE IT REMEMBERED that, pursuant to Notice, and
on Friday, the 4th day of March, 2022, commencing at the
hour of 9:03 a.m., thereof, in Sunnyvale, California,
before me, KATY E. SCHMIDT, a Certified Shorthand
Reporter in and for the County of Yolo, State of
California, there virtually personally appeared

WING PAN "BERT" LEUNG

called as a witness herein, who, being by me first duly
sworn, was thereupon examined and interrogated as
hereinafter set forth.

CONFIDENTIAL

1 APPEARANCES:

2 For The Plaintiffs:

3 (Appeared via Zoom)

4 BLEICHMAR FONTI & AULD LLP

BY: LESLEY WEAVER, Esq.

5 555 12th Street, Suite 1600

Oakland, California 994607

6 415.445.4003

lweaver@bfalaw.com

7 (Appeared via Zoom)

8 BOIES SCHILLER FLEXNER LLP

9 BY: MARK MAO, Esq.

BY: BEKO RICHARDSON, Esq.

10 BY: ERIKA NYBORG-BURCH, Esq.

44 Montgomery Street, 41st Floor

11 San Francisco, California 94104

415.293.6800

12 mmao@bsfllp.com

13 (Appeared via Zoom)

14 MORGAN & MORGAN

BY: RYAN MCGEE, Esq.

15 BY: RYAN YANCHUNIS, Esq.

201 North Franklin Street, Suite 700

16 Tampa, Florida 33602

813.223.0931

17 rmcgee@forthepeople.com

18 (Appeared via Zoom)

19 SUSMAN GODFREY LLP

BY: ALEXANDER FRAWLEY, Esq.

20 BY: AMANDA BONN, Esq.

1900 Avenue Of The Stars, Suite 1400

21 Los Angeles, California 90067-4405

310.789.3131

22 abonnn@susmangodfrey.com

23 ///

24 ///

25 ///

CONFIDENTIAL

1 APPEARANCES CONT.:

2 For The Defendants:

3 (Appeared via Zoom)

4 Quinn Emanuel Urquhart & Sullivan LLP

BY: JOSEF ANSORGE, Esq.

5 BY: CARL SPILLY, Esq.

51 Madison Avenue, 22nd Floor

6 New York, New York 10010

212.849.7000

7 josefansorge@quinnemanuel.com

8 Also present:

9 Sean Grant, Videographer

10 Matthew Gubiotti, In-house counsel

11 ---o0o---

CONFIDENTIAL

INDEX OF EXAMINATION

---o0o---

	Page
Examination by Mr. Mao	10
Examination by Mr. Ansorge	261
Examination by Mr. Mao	262

---o0o---

QUESTIONS INSTRUCTED NOT TO ANSWER

Page	Line
------	------

(NOTHING OFFERED.)

---o0o---

CONFIDENTIAL

1 BY MR. MAO: 09:22

2 Q. Okay. Have you ever seen this document 09:22

3 before? You may take the time to read it. 09:22

4 A. I'm not aware if I read this before. 09:22

5 Q. Got it. 09:22

6 Do you know whether or not you're going to 09:22

7 appear for an evidentiary hearing on April 21st of this 09:22

8 year? 09:22

9 A. Sorry. Can you repeat the question? 09:22

10 Q. Do you know -- yeah. Right. 09:23

11 Do you know whether or not you're going to 09:23

12 appear for an evidentiary hearing on April 21st of this 09:23

13 year? 09:23

14 MR. ANSORGE: Objection. Vague and 09:23

15 foundation. 09:23

16 THE WITNESS: I'm only aware of there were 09:23

17 initial -- some initial scheduling on February -- end of 09:23

18 February. I forgot which day that I rescheduled. 09:23

19 BY MR. MAO: 09:23

20 Q. So there was scheduling for February of this 09:23

21 year for what? What is it that you're aware of? 09:23

22 A. Deposition. 09:23

23 Q. Depositions. 09:23

24 You mean scheduling of your deposition for 09:23

25 sometime in February of this year? 09:23

Page 24

Page 25

CONFIDENTIAL

1 BY MR. MAO: 09:25

2 Q. Okay. Have you been keeping up with this 09:25

3 case? 09:25

4 MR. ANSORGE: Objection. Vague. 09:25

5 THE WITNESS: What do you mean by keeping up, 09:25

6 to which detail? 09:25

7 BY MR. MAO: 09:25

8 Q. When were you first brought in by Google to 09:25

9 support the Brown versus Google case, this case on 09:25

10 private browsing? 09:25

11 MR. ANSORGE: Objection. Form. 09:25

12 THE WITNESS: I've heard about a Brown case 09:25

13 probably a year ago or so. I forgot how long. 09:25

14 BY MR. MAO: 09:25

15 Q. Was that in 2021 or 2020 you were first -- you 09:25

16 first heard about the Brown case? 09:25

17 A. I don't recall exactly whether it's 2021 or 09:25

18 2020. Maybe 2020. 09:25

19 Q. Okay. And were you brought in by counsel or 09:25

20 were you brought in within just the Google engineering 09:25

21 team, the team that you were working with Mr. Liao? 09:25

22 MR. ANSORGE: Objection. Form. 09:26

23 And I want to caution the witness to the 09:26

24 extent the question is asking you to reveal privileged 09:26

25 attorney-client communications. Yeah. Please keep 09:26

Page 26

CONFIDENTIAL

1 A. As of that -- possibly those other production 11:54
2 logs -- those existing production logs, that is logs for 11:54
3 likely some ads traffic, and each of the logs I would 11:55
4 assume -- I would expect they would be certain retention 11:55
5 period for each of them. 11:55

6 Q. Okay. So other than looking at the logs, are 11:55
7 there other ways as to how we can tell when the 11:55
8 incognito bit went into production for the purposes of 11:55
9 logs? 11:55

10 MR. ANSORGE: Objection. Form and compound. 11:55

11 THE WITNESS: Can you clarify what do you 11:55
12 mean by this [REDACTED] bit going to 11:55
13 production? Do you mean started the computation, some 11:55
14 production server -- 11:55

15 BY MR. MAO: 11:55

16 Q. You say "We have been logging the fields for a 11:55
17 while"; right? 11:55

18 My question is: How do I know when you 11:55
19 started "been logging the fields for a while?" How do 11:56
20 I tell? 11:56

21 MR. ANSORGE: Objection. Vague. 11:56

22 THE WITNESS: First of all, if I remember 11:56
23 correctly, when I said in that conversation those fields 11:56
24 may be logging for a while, I do not mean to say I know 11:56
25 the start time, the first day those data are being 11:56

Page 102

CONFIDENTIAL

1 available. 11:56

2 And I do not mean those data will still -- all 11:56

3 those data will still keep preserve over the time 11:56

4 because that is control by certain log retention, which 11:56

5 is in force on the log itself, which is not under my 11:57

6 control. 11:57

7 What I mean in that conversation is those 11:57

8 data, which is the output of the -- for the computation, 11:57

9 which include the enum and the [REDACTED] 11:57

10 bit, could be in those production -- could be in some 11:57

11 production logs already at the time that conversation 11:57

12 happened. 11:57

13 BY MR. MAO:

14 Q. Were you ever told to preserve the incognito 11:57

15 bit in these production logs? 11:57

16 MR. ANSORGE: Objection. Vague. 11:57

17 THE WITNESS: Can you -- 11:57

18 BY MR. MAO: 11:57

19 Q. Let me clarify. 11:57

20 Were you ever told for the purposes of this 11:57

21 litigation to retain the logs that contain these 11:57

22 incognito bits? 11:58

23 A. As far as I remember, I was told to retain the 11:58

24 documentation regarding this project. 11:58

25 Q. Were you actually told to retain and preserve 11:58

Page 103

CONFIDENTIAL

1 the data for the purposes of this litigation? 11:58

2 MR. ANSORGE: Here I want to caution the 11:58

3 witness not to reveal attorney-client privileged 11:58

4 communications. 11:58

5 BY MR. MAO: 11:58

6 Q. You may answer. 11:58

7 A. I don't recall -- I'm not entirely sure 11:58

8 whether this is -- this would fall into the privileged 11:58

9 conversation so I probably need to consult the counsel 11:58

10 on this. 11:58

11 Q. Did you have any conversations, other than 11:59

12 with counsel, regarding whether or not data containing 11:59

13 the incognito bit should be preserved? 11:59

14 A. If this is a -- I don't recall the details, 11:59

15 again. As I said, this is just a tiny part of my daily 11:59

16 job. 11:59

17 I would assume, if there are ever any 11:59

18 conversation regarding this litigation and logs being 11:59

19 preserved, it should likely be with the counsel, I would 11:59

20 suppose, which as I said, I'm not entirely sure whether 11:59

21 this would be privileged or not. 11:59

22 Q. So other than with counsel, you do not recall 11:59

23 currently any conversations where you were told to 11:59

24 preserve this data. 11:59

25 Is that correct? 11:59

1	undertaking -- I'm sorry.	12:01
2	Did you say something, Mr. Ansorge?	12:01
3	MR. ANSORGE: I was just saying when you come	12:01
4	to a natural stop, it would be great for us to have that	12:01
5	lunch.	12:01
6	MR. MAO: Yeah. I'll be done with this area	12:01
7	soon.	12:01
8	BY MR. MAO:	12:01
9	Q. To the best of your recollection, did you	12:01
10	undertake any efforts to try to preserve data in this	12:01
11	case?	12:01
12	A. Can you clarify what data means?	12:01
13	Q. Okay. Were you involved in the preservation	12:01
14	of plaintiffs' data in this case?	12:02
15	A. First of all, I'm not entirely sure what do	12:02
16	you mean by retain information for this plaintiffs'	12:02
17	data.	12:02
18	As far as I recall, I did not delete any	12:02
19	documentation regarding of this project while in	12:02
20	reality, most of the time I don't -- I don't delete any	12:02
21	documentation regarding my design, regarding the	12:02
22	internal documentation at all.	12:02
23	Q. No. I'm talking about the production data.	12:02
24	The data you're talking about that you've been	12:02
25	logging here in this document, did you undertake any	12:02

CONFIDENTIAL

1 effort to preserve this data? 12:02

2 I'm not talking about conversations. I just 12:02

3 want to know whether or not you and Google undertook any 12:03

4 efforts to preserve this data? 12:03

5 MR. ANSORGE: Objection. Foundation. Form. 12:03

6 Asked and answered. 12:03

7 THE WITNESS: As far as I can tell -- and 12:03

8 first of all, again, I am not owning the logging 12:03

9 infrastructure, nor defining the retention period. 12:03

10 As far as I'm aware of, I'm not aware of any 12:03

11 change to the retention period of ads logs. 12:03

12 BY MR. MAO: 12:03

13 Q. Who owns the logging retention period for this 12:03

14 project, the part about adding the incognito bit into 12:03

15 the logs? Who would be responsible by Google for that? 12:03

16 MR. ANSORGE: Objection. Compound. 12:03

17 THE WITNESS: This project includes logging 12:03

18 certain outputs into the -- into the production logs. 12:04

19 But as I said earlier, the retention of the 12:04

20 production log, which include other data as well, is not 12:04

21 controlled by this project, nor my team. 12:04

22 BY MR. MAO:

23 Q. Okay. But the changes to the actual fields 12:04

24 here, right, that is owned by your team, isn't it? 12:04

25 MR. ANSORGE: Objection. Vague. 12:04

Page 107

CONFIDENTIAL

1 THE WITNESS: Can you define what do you mean 12:04
2 by those fields? Do you mean the output that I 12:04
3 mentioned earlier? Only the output related to this 12:04
4 project? 12:04
5 BY MR. MAO: 12:04
6 Q. Sure. 12:04
7 The output that you've been logging referred 12:04
8 to in your line here on October 27, 2021, right, the 12:04
9 output in, "We have been logging the fields for a while 12:05
10 already," is that owned by your team? 12:05
11 A. The logic to compute those output and to add 12:05
12 it to production log is only by my team. But the whole 12:05
13 ads log itself and also the whole -- the logging 12:05
14 infrastructure, they are not owned by my team. 12:05
15 Q. Okay. So with regard to the logic that you 12:05
16 own, okay, your team owns, did you take -- undertake any 12:05
17 efforts to preserve, okay, whatever data or 12:05
18 documentation you have as to when the logic changed? 12:05
19 The change in the logic so that you'd be logging these 12:05
20 additional fields or additional output, whatever you 12:06
21 want to call it. 12:06
22 MR. ANSORGE: Objection. Form, and compound. 12:06
23 THE WITNESS: Sorry. I got lost in the 12:06
24 question. Can you repeat your question? 12:06
25 ///

Page 108

CONFIDENTIAL

1 THE WITNESS: First of all, I don't recall 06:04
2 when was the first time that I've been in touch with 06:04
3 those lawyers. 06:04

4 Second, also it's because it's a very long 06:04
5 time ago, I don't even recall the context of that 06:04
6 conversation. 06:04

7 BY MR. MAO: 06:04

8 Q. Were you asked to find out that date in 06:04
9 preparation for this deposition by anybody? 06:04

10 A. I'm not aware of that. 06:04

11 Q. What about for the upcoming hearing, were you 06:04
12 asked by anybody to find out that date? 06:04

13 A. What do you mean by "upcoming hearing"? 06:04

14 Q. The upcoming hearing, were you asked by 06:04
15 anybody to figure out when you received the evidence 06:04
16 preservation letter? 06:04

17 A. So as far as I understand, upcoming hearing 06:04
18 means that doesn't happen yet. I'm not sure what 06:04
19 upcoming hearing you're talking about, so I'm not sure 06:05
20 how to answer your question. 06:05

21 Q. Right. So you're not -- you don't know. 06:05
22 Is that the answer? 06:05

23 MR. ANSORGE: Yeah. Objection. Asked and 06:05
24 answered. 06:05

25 And could I -- could we get a time count, 06:05

Page 260

CONFIDENTIAL

1 please? 06:05

2 THE VIDEOGRAPHER: 6:59. 06:05

3 MR. MAO: I'll pass it to you, Mr. Ansorge. 06:05

4 That's the record I will take. 06:05

5 MR. ANSORGE: Great. Thank you, Mr. Mao. 06:05

6 Thank you, Mr. Leung. 06:05

7 EXAMINATION BY MR. ANSORGE 06:05

8 BY MR. ANSORGE: 06:05

9 Q. Do you recall Mr. Mao asking you a series of 06:05

10 questions about the [REDACTED] bit? 06:05

11 A. Yes. 06:05

12 Q. Why is it called the [REDACTED] 06:05

13 bit? 06:05

14 A. Well, first of all, it's many times that 06:05

15 describing in this deposition is coming from a heuristic 06:05

16 approximation to identify those traffic. 06:05

17 So by adding that [REDACTED] prefix in the field, 06:06

18 make it even more clear that it's not a reliable signal, 06:06

19 it does not mean to be accurate. That's why adding that 06:06

20 prefix will just help to prevent misuse of this 06:06

21 information further by ad engineers. 06:06

22 Q. Is the [REDACTED] bit a signal 06:06

23 that is sent from an instance of the Chrome browser to 06:06

24 Google? 06:06

25 A. No. 06:06

Page 261

CONFIDENTIAL

1 Q. Is the [REDACTED] bit a definitive 06:06
2 or reliable signal to identify incognito mode? 06:06

3 A. No. 06:06

4 Q. Is the [REDACTED] bit a signal the 06:06
5 browser sends to [REDACTED]? 06:06

6 A. No. 06:06

7 Q. Are you aware of [REDACTED] using the 06:06
8 [REDACTED] field bit in any way? 06:06

9 A. I am not aware of any of that. 06:07

10 MR. ANSORGE: No further questions at this 06:07
11 time. 06:07

12 MR. MAO: I have a redirect. 06:07

13 FURTHER EXAMINATION BY MR. MAO 06:07

14 BY MR. MAO: 06:07

15 Q. Are you aware of [REDACTED] using the input which is 06:07
16 relied on by the [REDACTED] bit? 06:07

17 A. Which part of the input you are talking about? 06:07

18 Q. The input that goes into the incognito bit. 06:07

19 A. So as I mentioned earlier, that 06:07
20 [REDACTED] bit, the heuristic approximation 06:07
21 that is coming from more than one input; right? The 06:07
22 user agent, the presence of X-Client-Data header, for 06:07
23 example, I'm aware of user agent being part of the 06:08
24 information passing the [REDACTED], but I'm not aware of the 06:08
25 presence of X-Client-Data header being part of the 06:08

Page 262

CONFIDENTIAL

REPORTER'S CERTIFICATE

---o0o---

STATE OF CALIFORNIA)
) ss.

COUNTY OF YOLO)

I, KATY E. SCHMIDT, a Certified Shorthand
Reporter in and for the State of California, duly
commissioned and a disinterested person, certify:

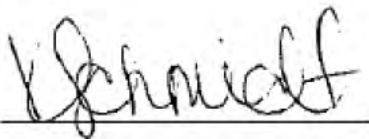
That the foregoing deposition was taken before me
at the time and place herein set forth;

That WING PAN "BERT" LEUNG, the deponent herein,
was put on oath by me;

That the testimony of the witness and all
objections made at the time of the examination were
recorded stenographically by me to the best of my
ability and thereafter transcribed into typewriting;

That the foregoing deposition is a record of the
testimony of the examination.

IN WITNESS WHEREOF, I subscribe my name on this
7th day of March, 2022.



Katy E. Schmidt, RPR, RMR, CRR, CSR 13096
Certified Shorthand Reporter in and for the
County of Sacramento, State of California

Page 266

EXHIBIT 40
Redacted Version of
Document Sought to
be Sealed

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

---o0o---

PATRICK CALHOUN, et al.,)
on behalf of themselves and)
all others similarly)
situated,)

Plaintiffs,

)Case No.

)5:20-cv-5146-LHK-SVK

vs.)

GOOGLE LLC,)

Defendant.)

-----)
CHASOM BROWN, et al.,)
on behalf of themselves and)
all others similarly)
situated,)

Plaintiffs,

)Case No.

)5:20-cv-03664-LHK

vs.)

GOOGLE LLC,)

Defendant.)

---o0o---

Videotaped Zoom Deposition of
HUEI-HUNG (CHRIS) LIAO
CONFIDENTIAL, ATTORNEYS' EYES ONLY
Friday, December 3, 2021

---o0o---

Katy E. Schmidt
RPR, RMR, CRR, CSR 13096
Veritext Job No.: 4962198

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

---o0o---

PATRICK CALHOUN, et al.,)
on behalf of themselves and)
all others similarly)
situated,)

Plaintiffs,

)Case No.

)5:20-cv-5146-LHK-SVK

vs.)

GOOGLE LLC,)

Defendant.)

CHASOM BROWN, et al.,)
on behalf of themselves and)
all others similarly)
situated,)

Plaintiffs,

)Case No.

)5:20-cv-03664-LHK

vs.)

GOOGLE LLC,)

Defendant.)

BE IT REMEMBERED that, pursuant to Notice, and
on Friday, the 3rd day of December, 2021, commencing at
the hour of 9:05 a.m., thereof, in Sunnyvale,
California, before me, KATY E. SCHMIDT, a Certified
Shorthand Reporter in and for the County of Yolo, State
of California, there virtually personally appeared
HUEI-HUNG (CHRIS) LIAO
called as a witness herein, who, being by me first duly
sworn, was thereupon examined and interrogated as
hereinafter set forth.

1 APPEARANCES:

2 For The Plaintiffs:

3 (Appeared via Zoom)

4 BLEICHMAR FONTI & AULD LLP

BY: LESLEY WEAVER, Esq.

5 555 12th Street, Suite 1600

Oakland, California 994607

6 415.445.4003

lweaver@bfalaw.com

7 (Appeared via Zoom)

8 SIMMONS HANLY CONROY

9 BY: JASON "JAY" BARNES, Esq.

BY: AN TRUONG, Esq.

10 One Court Street

Alton, Illinois 62002

11 618.693.3104

jaybarnes@simmonsfirm.com

12 (Appeared via Zoom)

13 BOIES SCHILLER FLEXNER LLP

14 BY: MARK MAO, Esq.

BY: BEKO RICHARDSON, Esq.

15 BY: ERIKA NYBORG-BURCH, Esq.

44 Montgomery Street, 41st Floor

16 San Francisco, California 94104

415.293.6800

17 mmao@bsfllp.com

18 For The Defendants:

19 (Appeared via Zoom)

20 Quinn Emanuel Urquhart & Sullivan LLP

BY: JOSEF ANSORGE, Esq.

21 BY: TRACY GAO, Esq.

51 Madison Avenue, 22nd Floor

22 New York, New York 10010

212.849.7000

23 josefansorge@quinnemanuel.com

24 ///

25 ///

1 APPEARANCES CONTINUED:

2 Also present:

3 David West, Videographer

4 Ryan McGee, In-house counsel

5 Toni Baker, In-house counsel

6

---o0o---

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

CONFIDENTIAL - ATTORNEYS' EYES ONLY

INDEX OF EXAMINATION

---o0o---

Page

Examination by Mr. Mao

09

Examination by Mr. Ansorge

197

---o0o---

QUESTIONS INSTRUCTED NOT TO ANSWER

Page Line

(NOTHING OFFERED.)

---o0o---

Page 5

CONFIDENTIAL - ATTORNEYS' EYES ONLY

1 A. Okay. I have it. 01:06

2 Q. This looks to me to basically be a variant of 01:06

3 your prior graph, I think. 01:07

4 You could take a look -- 01:07

5 A. It appears so. 01:07

6 Q. Yeah. 01:07

7 So my question to you, and I think -- I think 01:07

8 Mr. Barnes asked this, either from this graph or the 01:07

9 graph like you saw before on the other exhibit that was 01:07

10 right below this. 01:07

11 I think my question to you is -- I think -- 01:07

12 oh, yes. There, I see it. It's been grayed out. 01:07

13 You see on the top right, right under "Parse 01:07

14 PPID," there's a "Parse privacy req params"? 01:07

15 Again, I might be referring to the wrong one 01:07

16 of two graphs. But I believe that you said that that's 01:07

17 parsing whether or not the incoming signal from the 01:07

18 external world contains a privacy preference or setting 01:07

19 of some type. 01:07

20 Is that -- do I have that right? 01:08

21 MR. ANSORGE: Objection. Mischaracterizes 01:08

22 prior testimony. 01:08

23 THE WITNESS: For the box of "parse privacy 01:08

24 req," which stands for "request," parameters, the 01:08

25 purpose of this piece of logic is to parse the URL 01:08

1 parameters that are related to privacy treatment as we 01:08
2 receive from the URL network request itself. 01:08

3 As I stated yesterday, I believe some of the 01:08
4 examples of such a URL can be, for example, GDPR, which 01:08
5 indicates to our systems that applicable GDPR behaviors 01:08
6 have to be enabled for this particular ad query. 01:08

7 I believe another example I gave was TFCD, 01:08
8 which stands for "treat for child directed." I believe 01:09
9 the presence of the parameter enables our systems to 01:09
10 treat the ad query with the necessary child directed 01:09
11 treatments. 01:09

12 BY MR. MAO:

13 Q. Got it. Got it. 01:09

14 As far as you're aware, amongst these privacy 01:09
15 signals, is there one for incognito mode browsing on 01:09
16 Chrome? 01:09

17 A. No. 01:09

18 Q. Is there a reason that you're aware as to why 01:09
19 that would not be a privacy req parameter for [REDACTED]? 01:09

20 MR. ANSORGE: Objection. Form. 01:09

21 THE WITNESS: I am not aware of a URL 01:09
22 parameter that would indicate incognito mode. 01:09

23 BY MR. MAO: 01:09

24 Q. What about a parameter specifically to signal 01:09
25 to [REDACTED] to parse out that, oh, this is incognito mode 01:09

1 traffic? 01:10

2 A. There is no explicit signal to identify 01:10

3 incognito mode traffic. 01:10

4 Q. Were you ever involved in any discussions on 01:10

5 whether or not [REDACTED] should be designed to receive and 01:10

6 parse such a signal? 01:10

7 A. I was involved in projects having to work with 01:10

8 incognito mode. 01:10

9 Q. Was there a discussion on whether or not that 01:10

10 should be a signal to [REDACTED]? Whether or not that design 01:10

11 should include, you know, a signal to [REDACTED], saying that 01:10

12 the user or device was browsing in incognito mode? 01:10

13 A. I do not recall if there was a specific 01:10

14 discussion around using the URL parameter as a signal 01:10

15 to [REDACTED] to indicate incognito mode. 01:10

16 But as I stated, I was involved in projects 01:11

17 related to incognito mode. 01:11

18 Q. How about amongst those projects that you were 01:11

19 involved, were there any discussions on whether or not 01:11

20 there were any other types of signals other than a URL 01:11

21 parameter signal for incognito traffic that would be 01:11

22 given to [REDACTED] at the -- 01:11

23 MR. ANSORGE: Objection. 01:11

24 MR. MAO: Sorry. It was at the parsing layer, 01:11

25 Ms. Court Reporter. 01:11

CONFIDENTIAL - ATTORNEYS' EYES ONLY

1 Yeah. Go ahead, Joey, please. 01:11

2 MR. ANSORGE: Yeah. Objection. Vague. 01:11

3 THE WITNESS: Can you clarify which part of 01:11

4 ████ you're referring to in this question? 01:11

5 BY MR. MAO: 01:11

6 Q. Sure. Sure. 01:11

7 I'm looking at the parsing layer. And my 01:11

8 understanding of that is that that's the first layer 01:11

9 that kind of hits █████ that says, hey, here are all the 01:11

10 signals coming from the external world in which, you 01:11

11 know, like might be relevant, you know, for terms of 01:11

12 ████ digesting and then spitting out whatever it spits 01:11

13 out on the other end. 01:11

14 My question is -- you limited your prior 01:11

15 answers to a URL signal for █████ and you not being aware 01:12

16 of that being a discussion. 01:12

17 My question to you is whether or not you're 01:12

18 aware of a discussion or proposal on a non-URL signal 01:12

19 that would be sent to █████? 01:12

20 A. I do not recall the specifics of such a 01:12

21 discussion. I do not recall if such a discussion -- 01:12

22 specific discussion happened. 01:12

23 But as I stated, I was involved in projects 01:12

24 that have -- have to do with incognito mode. And there 01:12

25 was discussion around proxy signals that we can use to 01:12

REPORTER'S CERTIFICATE

---o0o---

STATE OF CALIFORNIA)
) ss.

COUNTY OF YOLO)

I, KATY E. SCHMIDT, a Certified Shorthand
Reporter in and for the State of California, duly
commissioned and a disinterested person, certify:

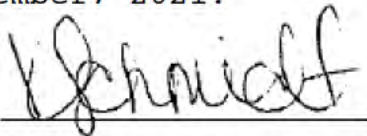
That the foregoing deposition was taken before me
at the time and place herein set forth;

That HUEI-HUNG (CHRIS) LIAO, the deponent herein,
was put on oath by me;

That the testimony of the witness and all
objections made at the time of the examination were
recorded stenographically by me to the best of my
ability and thereafter transcribed into typewriting;

That the foregoing deposition is a record of the
testimony of the examination.

IN WITNESS WHEREOF, I subscribe my name on this
6th day of December, 2021.



Katy E. Schmidt, RPR, RMR, CRR, CSR 13096
Certified Shorthand Reporter
in and for the
County of Sacramento,
State of California

Ref. No. 4962198 KES

EXHIBIT 41
Redacted Version of
Document Sought to
be Sealed

CONFIDENTIAL

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

---o0o---

CHASOM BROWN, et al.,)
on behalf of themselves and)
all others similarly)
situated,)

Plaintiffs,) Case No.

) 5:20-cv-03664-LHK

vs.)

GOOGLE LLC,)

Defendant.)

-----)

---o0o---

Videotaped Zoom Deposition of

MANDY LIU

CONFIDENTIAL

Tuesday, March 8, 2022

---o0o---

Katy E. Schmidt
RPR, RMR, CRR, CSR 13096
Job No.: 5121622

Page 1

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

---o0o---

CHASOM BROWN, et al.,)
on behalf of themselves and)
all others similarly)
situated,)
)
 Plaintiffs,)Case No.
)5:20-cv-03664-LHK
vs.)
)
GOOGLE LLC,)
)
 Defendant.)
_____)

BE IT REMEMBERED that, pursuant to Notice, and
on Tuesday, the 8th day of March, 2022, commencing at
the hour of 7:01 a.m., thereof, in Kitchener, Ontario,
before me, KATY E. SCHMIDT, a Certified Shorthand
Reporter in and for the County of Yolo, State of
California, there virtually personally appeared

MANDY LIU

called as a witness herein, who, being by me first duly
sworn, was thereupon examined and interrogated as
hereinafter set forth.

CONFIDENTIAL

1 APPEARANCES:

2 For The Plaintiffs:

3 (Appeared via Zoom)

4 BOIES SCHILLER FLEXNER LLP

BY: MARK MAO, Esq.

5 BY: BEKO RICHARDSON, Esq.

44 Montgomery Street, 41st Floor

6 San Francisco, California 94104

415.293.6800

7 mmao@bsfllp.com

8 (Appeared via Zoom)

9 SUSMAN GODFREY LLP

BY: ALEXANDER FRAWLEY, Esq.

10 1301 Avenue Of The Stars, 32nd Floor

New York, New York 10019

11 212.729.2044

afrawley@susmangodfrey.com

12 For The Defendants:

13 (Appeared via Zoom)

14 Quinn Emanuel Urquhart & Sullivan LLP

15 BY: JOSEF ANSORGE, Esq.

BY: CARL SPILLY, Esq.

16 51 Madison Avenue, 22nd Floor

New York, New York 10010

17 212.849.7000

josefansorge@quinnemanuel.com

18 Also present:

19 Sean Grant, Videographer

21 Matthew Gubiotti, In-house counsel

---o0o---

CONFIDENTIAL

INDEX OF EXAMINATION

---o0o---

	Page
Examination by Mr. Frawley	08
Examination by Mr. Ansorge	56
Examination by Mr. Frawley	58

---o0o---

QUESTIONS INSTRUCTED NOT TO ANSWER

Page	Line
------	------

(NOTHING OFFERED.)

---o0o---

CONFIDENTIAL

1 Does that work for you? 09:05

2 THE WITNESS: Yes. 09:05

3 MR. FRAWLEY: Okay. Does that work for you, 09:05

4 Joey? 09:05

5 MR. ANSORGE: Yeah. Just bearing in mind we 09:05

6 got that 1:00 o'clock Special Master thing. 09:05

7 So thank you, Mr. Frawley. Let's go off the 09:05

8 record. 09:05

9 THE VIDEOGRAPHER: Going off the record. The 09:05

10 time is 12:05 p.m. 09:05

11 (Break taken in proceedings.) 09:11

12 THE VIDEOGRAPHER: Back on the record. The 09:12

13 time is 12:12 p.m. 09:12

14 MR. FRAWLEY: Ms. Liu, I don't have any 09:12

15 further questions at this time. 09:12

16 Thank you. 09:12

17 THE WITNESS: Okay. 09:12

18 MR. ANSORGE: I'll have a few. 09:12

19 EXAMINATION BY MR. ANSORGE 09:12

20 BY MR. ANSORGE: 09:12

21 Q. Ms. Liu, could you please pull up Exhibit 4? 09:12

22 A. Yes, I'm -- 09:12

23 Q. Let me know once you have it. 09:12

24 Do you recall Mr. Frawley asking you a series 09:12

25 of questions about this document earlier today? 09:12

CONFIDENTIAL

1 A. Yes. 09:13

2 Q. Please go down to look at the second comment 09:13

3 from Mr. Ary Young. It's starting on the bottom of the 09:13

4 first page with the Bates number ending in 526. 09:13

5 Do you see that? 09:13

6 A. Yes. 09:13

7 Q. Do you see where Ary Young asks, quote, "We 09:13

8 can't detect with certainty," unquote? Do you see that? 09:13

9 A. Yes. 09:13

10 Q. Can you please read out your response to 09:13

11 Ary Young which you provided in that chat? 09:13

12 A. Sure. My response was, quote: 09:13

13 "No. We can't, that's mainly because the incognito 09:13

14 detection relies on the absence of ads X-Client-Data 09:13

15 header, but there are other cases where Chrome 09:13

16 doesn't send this header. For example, if the 09:13

17 browser hasn't received any experiment config yet 09:13

18 (go slash detect-incognito)" link, end quote. 09:14

19 Q. Ms. Liu, does the [REDACTED] 09:14

20 Boolean field detect incognito with certainty? 09:14

21 A. No. 09:14

22 MR. ANSORGE: No further questions at this 09:14

23 time. We reserve the right if Mr. Frawley has any 09:14

24 further questions. 09:14

25 MR. FRAWLEY: I think I have a couple of 09:14

CONFIDENTIAL

1 recross questions. 09:14

2 FURTHER EXAMINATION BY MR. FRAWLEY 09:14

3 BY MR. FRAWLEY: 09:14

4 Q. So we can stay on this exhibit, Exhibit 4. 09:14

5 Now, Ms. Liu, do you see where you wrote 09:14

6 "e.g., if the browser hasn't received any experiment 09:14

7 config yet"? 09:14

8 A. Yes. 09:14

9 Q. Do you know how often that happens? 09:14

10 MR. ANSORGE: Objection. Vague. 09:14

11 THE WITNESS: No. 09:14

12 BY MR. FRAWLEY: 09:14

13 Q. Did you ever do any research to figure out how 09:14

14 often that happens? 09:14

15 A. No. 09:15

16 Q. Okay. 09:15

17 MR. FRAWLEY: I actually think that's all I 09:15

18 have. 09:15

19 MR. ANSORGE: Thank you. 09:15

20 We're fine with going off the record, 09:15

21 Mr. Frawley, if you are. 09:15

22 And thank you, Ms. Liu. 09:15

23 THE VIDEOGRAPHER: This concludes today's 09:15

24 videotaped deposition of Mandy Liu. We are off the 09:15

25 record at 12:15 p.m. 09:15

CONFIDENTIAL

REPORTER'S CERTIFICATE

---o0o---

STATE OF CALIFORNIA)
) ss.

COUNTY OF YOLO)

I, KATY E. SCHMIDT, a Certified Shorthand
Reporter in and for the State of California, duly
commissioned and a disinterested person, certify:

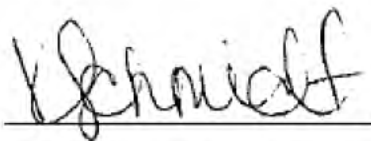
That the foregoing deposition was taken before me
at the time and place herein set forth;

That MANDY LIU, the deponent herein, was put on
oath by me;

That the testimony of the witness and all
objections made at the time of the examination were
recorded stenographically by me to the best of my
ability and thereafter transcribed into typewriting;

That the foregoing deposition is a record of the
testimony of the examination.

IN WITNESS WHEREOF, I subscribe my name on this
8th day of March, 2022.



Katy E. Schmidt, RPR, RMR, CRR, CSR 13096
Certified Shorthand Reporter
in and for the
County of Sacramento,
State of California

Ref. No. 5121622 KES

Page 60

EXHIBIT 42
Redacted Version of
Document Sought to
be Sealed

CONFIDENTIAL

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

---o0o---

CHASOM BROWN, et al.,)
on behalf of themselves and)
all others similarly)
situated,)

Plaintiffs,) Case No.

) 5:20-cv-03664-LHK

vs.)

GOOGLE LLC,)

Defendant.)

-----)

---o0o---

Videotaped Zoom Deposition of

DR. CAITLIN SADOWSKI

CONFIDENTIAL

Thursday, March 10, 2022

---o0o---

Katy E. Schmidt
RPR, RMR, CRR, CSR 13096
Veritext Job No.: 5130524

Page 1

---o0o---

DR. CAITLIN SADOWSKI

Page 2

CONFIDENTIAL

1 APPEARANCES:

2 For The Plaintiffs:

3 (Appeared via Zoom)

4 BOIES SCHILLER FLEXNER LLP

BY: MARK MAO, Esq.

5 BY: BEKO RICHARDSON, Esq.

44 Montgomery Street, 41st Floor

6 San Francisco, California 94104

415.293.6800

7 mmao@bsfllp.com

8 (Appeared via Zoom)

9 MORGAN & MORGAN

BY: RYAN MCGEE, Esq.

10 201 North Franklin Street, Suite 700

Tampa, Florida 33602

11 813.223.0931

rmcgee@forthepeople.com

12 For The Defendants:

13 (Appeared via Zoom)

14 QUINN EMANUEL URQUHART & SULLIVAN LLP

15 BY: JOSEF ANSORGE, Esq.

51 Madison Avenue, 22nd Floor

16 New York, New York 10010

212.849.7000

17 josefansorge@quinnemanuel.com

18 Also present:

19 Chad Given, Videographer

20 Toni Baker, In-house counsel

21 ---o0o---

CONFIDENTIAL

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

INDEX OF EXAMINATION

---o0o---

Page

Examination by Mr. McGee

08

---o0o---

QUESTIONS INSTRUCTED NOT TO ANSWER

Page Line

(NOTHING OFFERED.)

---o0o---

Page 4

Page 69

CONFIDENTIAL

1 [REDACTED] is 05:59
2 a binary field that is specifically used only in temp 05:59
3 [REDACTED] logs. 05:59
4 BY MR. MCGEE: 05:59
5 Q. And why is it only in temp [REDACTED] logs? 05:59
6 A. It was a field that was created by the [REDACTED] 06:00
7 team to help them understand potential problems with 06:00
8 their product location and where searching so that they 06:00
9 could develop the best product possible for Google 06:00
10 users. 06:00
11 Q. Okay. And it -- there's a note here that it 06:00
12 was introduced in 2017, but then the project wrapped up 06:00
13 in June of 2018. 06:00
14 Is that binary field still implemented at 06:00
15 Google? 06:00
16 MR. ANSORGE: Objection. Vague. 06:00
17 THE WITNESS: That binary field is -- still 06:00
18 exists as a binary field in and only in [REDACTED] logs. 06:00
19 BY MR. MCGEE: 06:01
20 Q. Are values written to that binary field in 06:01
21 [REDACTED] logs? 06:01
22 A. Yes. I believe values are written to that 06:01
23 binary field in [REDACTED] logs. 06:01
24 Q. So even though the project wrapped in June of 06:01
25 2018, that is still an actively used binary field? 06:01

Page 70

CONFIDENTIAL

1 MR. ANSORGE: Objection. Form. 06:01

2 THE WITNESS: As I understand it, it is not 06:01

3 actively used. It is still being written. It is not 06:01

4 being reviewed. 06:01

5 BY MR. MCGEE: 06:01

6 Q. Can you please clarify what you mean by "not 06:01

7 being reviewed"? 06:01

8 A. So from talking to Quentin, this field went 06:02

9 into a particular dashboard that the [REDACTED] team used 06:02

10 to identify situations where they are not getting a 06:02

11 location header but should be getting a location header. 06:02

12 And if a -- in situations where an X-Client-Data header 06:02

13 is not sent, they would also expect a location header to 06:02

14 not be sent in most situations like that. 06:02

15 So if there is an X-Client-Data header but 06:02

16 there's no location header, then that's potentially 06:02

17 indicative of a bug in the system. 06:02

18 So they have a dashboard that shows, you know, 06:02

19 how often that occurs and they could look at to, you 06:02

20 know, minimize the amount of times where a location 06:02

21 header should be sent but isn't sent. And they use that 06:03

22 dashboard to improve the product in this 2017-2018 time 06:03

23 range. 06:03

24 And from talking to Quentin, my understanding 06:03

25 is there's -- they're not actually looking at that 06:03

Page 71

CONFIDENTIAL

1 particular graph anymore in the normal course of 06:03
2 operations for the team. 06:03
3 Q. But if they pulled up the graph, there would 06:03
4 be responsive data that would fill in the graph; 06:03
5 correct? 06:03
6 MR. ANSORGE: Objection. Vague, and calls for 06:03
7 a legal conclusion. 06:03
8 THE WITNESS: I don't know what you mean by 06:03
9 responsive data that would fill in the graph. 06:03
10 BY MR. MCGEE: 06:03
11 Q. Sure. 06:03
12 So you're saying they aren't looking at the 06:03
13 graph anymore. They're not reviewing it. 06:03
14 What I'm asking is: Is if they did pull up 06:04
15 the graph, the graph would still have lines or bars or 06:04
16 whatever visual representation or graphical 06:04
17 representation the graph was designed to display. 06:04
18 Is that fair? 06:04
19 MR. ANSORGE: Objection. Compound. Form. 06:04
20 THE WITNESS: My understanding is that [REDACTED] 06:04
21 [REDACTED] 06:04
22 [REDACTED] is a field that is being filled in in 06:04
23 UMA -- not UMA -- not in UMA logs. It is not in UMA 06:04
24 logs, to be clear. It is only in [REDACTED] logs. And it 06:04
25 is a field that is still being filled in in [REDACTED] logs 06:04

Page 72

CONFIDENTIAL

1 today, despite the fact that the reason the field was 06:04
2 introduced has passed. 06:04
3 BY MR. MCGEE: 06:05
4 Q. Okay. And from your fact sheet, the 06:05
5 [REDACTED] 06:05
6 [REDACTED] -- so without the [REDACTED] -- 06:05
7 THE COURT REPORTER: I'm so sorry, Counsel. 06:05
8 Can you start that question over? There was a little 06:05
9 bit of feedback. I didn't get it. 06:05
10 MR. MCGEE: Sure. 06:05
11 BY MR. MCGEE:
12 Q. So the -- you've got two bullet points in your 06:05
13 fact sheet. 06:05
14 One is the [REDACTED] 06:05
15 [REDACTED], no GAIA. 06:05
16 What does that mean? 06:05
17 A. What that means is that the -- these [REDACTED] 06:05
18 logs that have this field set are not GAIA keyed. They 06:05
19 have location information. And then this is a Boolean 06:05
20 field, so it would be true or false. And there's the 06:06
21 location information, plus the Boolean field in the 06:06
22 [REDACTED] temp logs. 06:06
23 Q. Got it. 06:06
24 A. And not -- notably not GAIA IDs. 06:06
25 Q. Understood. 06:06

Page 73

CONFIDENTIAL

1 combine this with UMA data. 06:08

2 MR. MCGEE: I think we've been going for about 06:08

3 40 minutes now. I just need to take a break so -- 06:08

4 MR. ANSORGE: Yeah. I'm fine with that. 06:08

5 Could we get a time count as well? How much 06:08

6 time is left on the record? 06:08

7 THE VIDEOGRAPHER: Yeah. So off the record? 06:08

8 MR. MCGEE: Yes. Off the record. 06:08

9 THE VIDEOGRAPHER: Okay. We're now going off 06:08

10 the record. The time is 6:08 p.m. 06:08

11 (Break taken in proceedings.) 06:17

12 THE VIDEOGRAPHER: We are now back on the 06:17

13 record. The time is 6:18 p.m. 06:17

14 BY MR. MCGEE: 06:18

15 Q. Dr. Sadowski, for the bits that we were -- or 06:18

16 excuse me -- the binary fields that we were just talking 06:18

17 about, the [REDACTED] 06:18

18 [REDACTED], [REDACTED] 06:18

19 [REDACTED], and 06:18

20 [REDACTED], do you know 06:18

21 what logic is being used to derive the values that are 06:18

22 stored in those binary fields? 06:18

23 MR. ANSORGE: Objection. Vague and compound. 06:18

24 THE WITNESS: I believe the [REDACTED] 06:18

25 [REDACTED] is referring 06:18

Page 75

CONFIDENTIAL

1 to the same thing as [REDACTED] 06:18

2 [REDACTED]. I do know about 06:18

3 how that field is filled in. 06:19

4 BY MR. MCGEE: 06:19

5 Q. Okay. And what's the logic for filling in 06:19

6 that field? 06:19

7 A. It looks specifically at whether there is an 06:19

8 X-Client -- X hyphen Client hyphen Data header in the 06:19

9 request that is sent. 06:19

10 Q. Is there any other thing that it looks for or 06:19

11 is that all that it looks for? 06:19

12 A. I believe that is all that it looks for. The 06:19

13 [REDACTED] 06:19

14 [REDACTED] is if there is a X-Client-Data -- 06:19

15 X-Client-Data header sent, then that is the logic used 06:20

16 to set that to true. 06:20

17 This is a proxy for incognito, but it is not 06:20

18 a what I would call a reliable or accurate way to 06:20

19 determine incognito usage. 06:20

20 Q. Okay. And what's the -- what types of traffic 06:20

21 is this logic being applied to? Is it mobile traffic? 06:20

22 Is it -- you know, is it platform specific? 06:20

23 MR. ANSORGE: Objection. Vague and compound. 06:20

24 THE WITNESS: It is in [REDACTED] logs which are 06:21

25 [REDACTED]. I believe it will be 06:21

Page 76

CONFIDENTIAL

1 cross-platform, but I do not know for certain. I would 06:21
2 have to investigate. 06:21
3 BY MR. MCGEE:
4 Q. Who would you speak with at Google to 06:21
5 investigate that? 06:21
6 A. I would speak again with Quentin Fiard if I 06:21
7 had a question about the -- this particular field in 06:21
8 [REDACTED] logs. 06:21
9 Q. Okay. And then I did this backwards but -- 06:21
10 apologies. 06:21
11 I can -- I've introduced two new exhibits. 06:21
12 They're going to be 16 and 15. 06:22
13 (Plaintiffs' Exhibits 15 and 16 06:22
14 were marked for identification.) 06:22
15 BY MR. MCGEE: 06:22
16 Q. But I'd actually like you to look at 16 first. 06:22
17 A. 16 first? Okay. I'm waiting for it to load. 06:22
18 Q. Thank you. 06:22
19 A. One other thing to answer your question. 06:22
20 To the best of my knowledge the [REDACTED] 06:22
21 [REDACTED] field is derived from the 06:22
22 [REDACTED] 06:22
23 [REDACTED]. It is still depending on X-Client-Data 06:22
24 header logic and also looking at the user agent, but it 06:22
25 is not derived through some other mechanism than 06:22

Page 77

CONFIDENTIAL

1 A. No. 06:46

2 Q. But you did run the other one. And is that 06:46

3 how the list of log sources was populated in this 06:46

4 Exhibit 2 for Notice 2, Topic 10? 06:46

5 A. The way that the -- 06:46

6 MR. ANSORGE: Objection. Vague. 06:46

7 THE WITNESS: The list -- the bulleted list in 06:46

8 Notice 2, Topic 10 were populated by Quentin Fiard. 06:46

9 BY MR. MCGEE:

10 Q. Okay. But when you ran the [REDACTED] 06:46

11 [REDACTED] -- when you ran [REDACTED] -- you 06:46

12 did -- let me ask it this way: 06:47

13 You did a lot of -- or you did a few internal 06:47

14 code search queries; right? 06:47

15 A. Yes. 06:47

16 I would also like to note that in the course 06:47

17 of my job, I frequently run internal code search 06:47

18 queries. 06:47

19 Q. Okay. 06:47

20 A. I did a couple code search queries in 06:47

21 preparation for this case, either yesterday or this 06:47

22 morning. It has blended together and I'm not sure 06:47

23 which. But I make queries in code search in the normal 06:47

24 course of my job. 06:47

25 Q. Okay. And one of those queries returned 06:48

Page 90

CONFIDENTIAL

1 results; right? 06:48

2 A. Yes. If you search for [REDACTED] 06:48

3 [REDACTED], that substring is part of a 06:48

4 name of a Boolean field in [REDACTED] logs that I have 06:48

5 already testified about. And that binary field is using 06:48

6 X-Client-Data header information to proxy incognito 06:48

7 states. It is not an accurate name for the binary 06:48

8 field, and it is not used in UMA logs. 06:49

9 Q. Okay. I think I am -- very close. Just want 06:49
10 to make sure. 06:49

11 Does the [REDACTED] 06:49

12 [REDACTED] bit exist in 06:49

13 non-[REDACTED] logs? 06:49

14 A. To the best of my knowledge, that is the only 06:49

15 place it exists. If you -- this particular binary field 06:49

16 was developed with -- in -- as part of the design doc 06:50

17 that we reviewed earlier so that the [REDACTED] team could 06:50

18 look at how often they don't get a location header when 06:50

19 they're expecting to get a location header using the 06:50

20 presence -- or using the presence of the X-Client -- 06:50

21 presence or absence of the X-Client-Data header as a 06:50

22 proxy here for situations when you would or wouldn't 06:50

23 expect to get a location header. 06:50

24 Q. I understand that. 06:50

25 A. And that is the only way it is being used, to 06:50

Page 91

CONFIDENTIAL

1 my knowledge. 06:50

2 Q. And what is the basis of your knowledge for -- 06:50

3 what's the basis of your knowledge for that conclusion? 06:50

4 A. A few different things. 06:51

5 Talking to Quentin Fiard who was involved in 06:51

6 actually implementing this field. 06:51

7 Looking in code search, including historical 06:51

8 code search, for where this field is set and used. 06:51

9 And also if you look in the protocol buffer 06:51

10 that has this field, there is an annotation saying that 06:51

11 it is specifically only used in [REDACTED] logs. 06:51

12 And that there's also a comment that links to 06:51

13 the design doc that we talked about earlier that is 06:51

14 related to this field. 06:51

15 Q. And that comment is on an internal document at 06:51

16 Google? 06:51

17 A. It is a source code comment. 06:51

18 Q. Okay. 06:52

19 A. Not a document comment. And it is a comment 06:52

20 directly above the definition of this field. 06:52

21 MR. MCGEE: Okay. I don't have any further 06:52

22 questions. 06:52

23 Thank you. 06:52

24 MR. ANSORGE: We'd like to take a break to see 06:52

25 if we have any questions. 06:52

Page 92

CONFIDENTIAL

REPORTER'S CERTIFICATE

---o0o---

STATE OF CALIFORNIA)
) ss.

COUNTY OF YOLO)

I, KATY E. SCHMIDT, a Certified Shorthand
Reporter in and for the State of California, duly
commissioned and a disinterested person, certify:

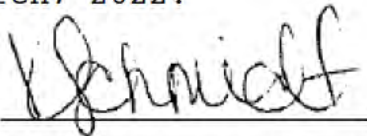
That the foregoing deposition was taken before me
at the time and place herein set forth;

That DR. CAITLIN SADOWSKI, the deponent herein,
was put on oath by me;

That the testimony of the witness and all
objections made at the time of the examination were
recorded stenographically by me to the best of my
ability and thereafter transcribed into typewriting;

That the foregoing deposition is a record of the
testimony of the examination.

IN WITNESS WHEREOF, I subscribe my name on this
11th day of March, 2022.



Katy E. Schmidt, RPR, RMR, CRR, CSR 13096
Certified Shorthand Reporter
in and for the
County of Sacramento,
State of California

Ref. No. 5130524 KES

Page 95

EXHIBIT 43

CHASOM BROWN, ET AL. versus GOOGLE, LLC, ET AL.
Hearing on 03/05/2022

1 UNITED STATES DISTRICT COURT
2 NORTHERN DISTRICT OF CALIFORNIA
3 CASE NO.: 4:20-03664-YGR-AVK
4
5 CHASOM BROWN, MARIA NGUYEN and
6 WILLIAM BYATT, individually and on
7 Behalf of all other similarly situated,
8 Plaintiffs,
9 versus
10 GOOGLE, LLC and ALPHABET, INC.,
11 Defendants.
12 _____/

13 TRANSCRIPT OF CIVIL CONTEMPT HEARING

14 DATE: March 5, 2022
15 PLACE: Remotely via Zoom
16 BEFORE: Special Master Douglas Brush
17
18
19

20 These proceedings were digitally recorded and the
21 following was transcribed by:

22 Denise D. Wilcox
23 Court Reporter/Transcriptionist
24 King Reporting
25 A Huseby Company
14 Suntree Place, #101
Melbourne, Florida 32940
(321) 242-8080

CHASOM BROWN, ET AL. versus GOOGLE, LLC, ET AL.
Hearing on 03/05/2022

Page 2

1 A-P-P-E-A-R-A-N-C-E-S

2

FOR THE PLAINTIFFS:

3

JASON "JAY" BARNES, ESQUIRE

4

Simmons, Hanly & Conroy

112 Madison Avenue, 7th Floor

5

New York, New York 10016

618-693-3104

6

MARK C. MAO, ESQUIRE

7

Boies, Schiller & Flexner, LLP

44 Montgomery Street, 41st Floor

8

San Francisco, California 94104

415-293-6800

9

10 FOR THE DEFENDANT GOOGLE, LLC:

11 STEPHEN A. BROOME, ESQUIRE

Quinn, Emanuel, Urquhart & Sullivan, LLP

12

865 South Figueroa Street, 10th Floor

Los Angeles, California 90017

13

213-443-3000

14 JOSEF ANSORGE, ESQUIRE

Quinn, Emanuel, Urquhart & Sullivan, LLP

15

1300 L Street Northwest, Suite 900

Washington, D.C. 20005

16

17 ALSO PRESENT:

18 TRACY GAO, Law Clerk at Quinn, et al

TIMOTHY SCHMIDT

19

DAVID STRAITE

20

21

22

23

24

25

CHASOM BROWN, ET AL. versus GOOGLE, LLC, ET AL.
Hearing on 03/05/2022

Page 66

1 produced the 100 fields, I think we sat -- there's
2 a portion of that that's a little bit of a
3 bombshell, which I don't think is necessary in --
4 in this current session, but we want to make sure
5 that those six types of fields are actually
6 produced for all the schema identified. Right.
7 Like, that's what we're trying to figure out,
8 because it does go to identifiability and join
9 ability. That's why. And we -- and in our
10 defense, Special Master, we've laid this out pretty
11 clearly ever since December.

12 MR. MCGEE: Right. And Special Master Brush,
13 there's -- there's one or two bits that, you know,
14 we continue to look at and that continue to peak
15 our interests, but they don't fall with this --
16 within this 100, and Google says, "Sorry, it's just
17 going to be too hard."

18 I -- there's got to be a way to craft a search
19 where we can get -- and where we can get this
20 information. I mean, it exists on their servers.
21 Just because it's not in the top 100, doesn't mean
22 that we should not be entitled to it.

23 (Whereupon, there were overlapping speakers.)

24 SPECIAL MASTER BRUSH: In the interest of
25 time, we're short now, so what I want to throw this

CHASOM BROWN, ET AL. versus GOOGLE, LLC, ET AL.
Hearing on 03/05/2022

Page 67

1 to is to Google's counsel. Do you understand
2 there's a bit of a dilemma there of we are all
3 trying to craft more or refine searches to reduce
4 the workload on both Google systems and engineers.

5 What do you propose is the best way to provide
6 better insight that allows more targeted searching
7 that will aid this. You know, as opposed -- you
8 know, maybe it was my fault for saying --
9 [indiscernible] -- produce these top hundred hoping
10 that was going to be enough. Clearly, we need to
11 refine things.

12 What would Google recommend, knowing their
13 systems better than anybody else, how we refine
14 some of these searches?

15 MR. MAO: So, if there's an option for a
16 specific refinement, the easiest way to do it would
17 be to focus on very specific fields, and I want to
18 be clear that that's different from the six
19 categories that Plaintiffs were referring to just
20 now. I mean, those -- when they state everything
21 that has an IP address, that -- that's not a
22 specific field.

23 So, if we have a field and an ID, and a time
24 period, those searches, of course, become much more
25 narrow and targeted. I should add that we've been

CHASOM BROWN, ET AL. versus GOOGLE, LLC, ET AL.
Hearing on 03/05/2022

Page 68

1 proceeding so far by just providing, you know, all
2 the information that would be keyed to the
3 particular ID in that storage.

4 So, this would be smaller and more focused;
5 however, what we have been doing so far also covers
6 the requirement that Plaintiffs have of some kind
7 of an organization or schema, because when they
8 received the data, they receive it by the different
9 field names that exist for that record, and so it
10 serves double purpose, without having to be
11 sequential and us having to follow one or the
12 other.

13 So, what we are proposed is maintain the
14 process we have had so far for the searches that
15 are under way for the next iteration of searches
16 that Plaintiffs provide. If we need a very quick
17 test account search, we narrow it and focus the
18 searches down to ID, URL, specific IP address of
19 the device, and user agent, the key fields that are
20 identified in the complaint. Following those
21 parameters will make it much more difficult. It
22 also doesn't run the risk of pulling in any
23 publisher data, so it slows down the entire end of
24 -- or negates the notification process, and that
25 would be our proposal on how to proceed.

CHASOM BROWN, ET AL. versus GOOGLE, LLC, ET AL.
Hearing on 03/05/2022

Page 111

1 STATE OF VIRGINIA)
2 COUNTY OF ROCKBRIDGE)

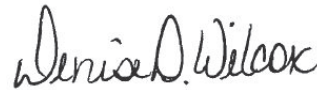
3 I, DENISE D. WILCOX, Court Reporter and
4 Digital Transcriptionist, do hereby certify that I
5 was authorized to and did transcribe the foregoing
6 proceeding from a digital audio recording, Brown v,
7 Google, and pages 1-111 of the transcript are a
8 true and correct record of the proceeding to the
9 best of my ability.

10

11 DONE AND DATED this 8th day of March,
12 2022, at Goshen, Rockbridge County, Virginia.

13

14



15

16

DENISE D. WILCOX
Court Reporter &
Digital Transcriptionist

17

18

19

20

21

22

23

24

25

EXHIBIT 44

1 DURIE TANGRI LLP
JOSEPH C. GRATZ (SBN 240676)
2 jgratz@durietangri.com
JOYCE C. LI (SBN 323820)
3 jli@durietangri.com
217 Leidesdorff Street
4 San Francisco, CA 94111
Telephone: 415-362-6666
5 Facsimile: 415-236-6300

6 Attorneys for Non-Party
MOZILLA CORPORATION
7
8
9
10

11 IN THE UNITED STATES DISTRICT COURT
12 FOR THE NORTHERN DISTRICT OF CALIFORNIA
13 SAN JOSE DIVISION

14 CHASOM BROWN, MARIA NGUYEN,
WILLIAM BYATT, JEREMY DAVIS, and
15 CHRISTOPHER CASTILLO, individually and on
16 behalf of all others similarly situated,

17 Plaintiffs,

18 v.

19 GOOGLE LLC,

20 Defendant.
21
22
23
24
25
26
27
28

Case No. 5:20-CV-03664-LHK-SVK

**NON-PARTY MOZILLA CORPORATION'S
OBJECTIONS AND RESPONSE TO
SUBPOENA TO PRODUCE DOCUMENTS,
INFORMATION OR OBJECTS**

Pursuant to Rule 45 of the Federal Rules of Civil Procedure and any other applicable rules of law, Non-party Mozilla Corporation (“Mozilla”) responds and objects to Plaintiffs Chasom Brown, Maria Nguyen, William Byatt, Jeremy Davis, and Christopher Castillo’s (collectively, “Plaintiffs”) Document Request attached to its Subpoena to Produce Documents, Information, or Objects or to Permit Inspection of Premises in a Civil Action (“Subpoena”) in the litigation styled *Chasom Brown, et al. v. Google, LLC*, Case No. 5:20-cv-03664 (N.D. Cal.) (the “Action”).

PRELIMINARY STATEMENT

Mozilla responds and objects based on its present knowledge. It reserves objections relating to any additional discovery and reserves the right to supplement, amend, or modify these objections and response.

GENERAL OBJECTIONS

Mozilla asserts the following objections as to the Subpoena and each and every Request:

1. Mozilla objects to the Subpoena and each and every Request to the extent that it seeks the production of documents or information protected by the attorney-client privilege, the work-product doctrine, the common interest privilege, or any other doctrine foreclosing compelled discovery. Nothing contained in these objections is intended as, or shall in any way be deemed, a waiver of any attorney-client privilege, attorney work-product protection, common interest privilege, or any other applicable privilege or doctrine. Mozilla will not provide information protected by any applicable privilege. Any disclosure of such information, inadvertent or otherwise, shall not be deemed a waiver of such protections.

2. Mozilla objects to the Subpoena and each and every Request to the extent it demands production of confidential or proprietary information including, without limitation, trade secrets. Mozilla will produce documents concerning such information only in accordance with any protective order in the Action.

3. Mozilla objects to the Subpoena and each and every Request to the extent any part of it seeks to impose on Mozilla obligations greater than those provided by law.

4. Mozilla objects to the Subpoena and each and every Request to the extent that it purports to impose a burden of providing information not in Mozilla’s possession, custody, or control or which

1 cannot be found in the course of a reasonable search.

2 5. Mozilla objects to the Subpoena and each and every Request to the extent it seeks
3 restoration or de-archiving of data not readily accessible in the ordinary course of business.

4 6. A representation that Mozilla will produce copies of non-privileged, responsive
5 documents that are within its possession, custody, or control is not a representation that any such
6 documents exist.

7 8. The fact that Mozilla has responded to part or all of a Request is not intended to and shall
8 not be construed as a waiver by Mozilla of any objection to such Request.

9 9. Mozilla's response and objections do not constitute any agreement by Mozilla with any of
10 the Definitions set forth in the Requests. To the extent Mozilla uses those Definitions, it does so only for
11 purposes of clarity and consistency.

12 10. Mozilla objects to the Definitions and Instructions to the extent they (i) are vague or
13 ambiguous; (ii) are overly broad or unduly burdensome; (iii) are inconsistent with the ordinary meaning
14 of the words or phrases they purport to define; (iv) seek to impose obligations different from or beyond
15 those required under the Federal Rules of Civil Procedure, under the Local Rules for the Northern
16 District of California, or by this Court; (v) include assertions of purported fact that are inaccurate or
17 disputed by Mozilla or the parties to the Action; or (vi) incorporate other Definitions or Instructions that
18 have these defects. In responding, Mozilla will adhere to the applicable rules, not to the Definitions and
19 Instructions.

20 11. All of these general objections are incorporated into each individual response set forth
21 below. The responses below are made subject to and without waiving these general objections.

22 **SPECIFIC OBJECTIONS TO REQUEST FOR PRODUCTION**

23 **REQUEST FOR PRODUCTION NO. 1:**

24 ALL DOCUMENTS sufficient to IDENTIFY all individuals who have used a Private Window or
25 Private Browsing mode in Firefox from June 1, 2016 to the present.

26 **RESPONSE TO REQUEST FOR PRODUCTION NO. 1:**

27 In addition to its General Objections, Mozilla objects to this Request on the grounds that it is
28 overbroad, unduly burdensome, and seeks discovery neither relevant to the claims or defenses of any

1 party nor proportional to the needs of the Action.

2 Mozilla also objects to this Request as overbroad to the extent it seeks “ALL DOCUMENTS
3 sufficient to IDENTIFY all individuals” and relies on Plaintiffs’ definition of “IDENTIFY.”

4 Mozilla also objects to this Request as unduly burdensome to the extent it seeks information that
5 is in the possession, custody, or control of the parties in the Action or is available from public sources.

6 Mozilla also objects to this Request to the extent it seeks information protected by the attorney-
7 client privilege, work-product doctrine, or common interest privilege or any other applicable privilege or
8 immunity.

9 Mozilla also objects to this request as calling for the production of private and confidential
10 information of third-party users without adequate justification.

11 In light of its objections, Mozilla responds as follows: Mozilla does not possess documents or
12 information sufficient to ascertain the identity of individuals who have used a Private Window or Private
13 Browsing mode in Firefox. In view of the foregoing, Mozilla will not be producing any documents.

14
15 Dated: August 27, 2021

DURIE TANGRI LLP

16
17 By: /s/ Joseph C. Gratz
JOSEPH C. GRATZ

18
19 Attorneys for Non-Party MOZILLA CORPORATION
20
21
22
23
24
25
26
27
28

PROOF OF SERVICE

I am employed in San Francisco County, State of California, in the office of a member of the bar of this Court, at whose direction the service was made. I am over the age of eighteen years, and not a party to the within action. My business address is 217 Leidesdorff Street, San Francisco, CA 94111.

On August 27, 2021, I served the following documents in the manner described below:

NON-PARTY MOZILLA CORPORATION'S OBJECTIONS AND RESPONSE TO SUBPOENA TO PRODUCE DOCUMENTS, INFORMATION OR OBJECTS



BY ELECTRONIC SERVICE: By electronically mailing a true and correct copy through Durie Tangri's electronic mail system from mrubalcaba@durietangri.com to the email addresses set forth below.

On the following part(ies) in this action:

Mark C. Mao
Sean P. Rodriguez
Beko Richardson
BOIES SCHILLER FLEXNER LLP
44 Montgomery St., 41st Floor
San Francisco, CA 94104
Tel: (415) 293-6800
Fax: (415) 293-6899
mmao@bsflp.com
srodriguez@bsflp.com
brichardson@bsflp.com

James Lee (*Pro Hac Vice*)
Rossana Baeza (*Pro Hac Vice*)
BOIES SCHILLER FLEXNER LLP
100 SE 2d St., 28th Floor
Miami, FL 33131
Tel: (305) 539-8400
Fax: (303) 539-1307
jlee@bsflp.com
rbaeza@bsflp.com

Amanda K. Bonn
SUSMAN GODFREY L.L.P.
1900 Avenue of the Stars, Suite 1400
Los Angeles, CA. 90067
Tel: (310) 789-3100
Fax: (310) 789-3150
abonn@susmangodfrey.com

William S. Carmody (*Pro Hac Vice*)
Shawn Rabin (*Pro Hac Vice*)
Steven M. Shepard (*Pro Hac Vice*)
SUSMAN GODFREY L.L.P.
1301 Avenue of the Americas, 32nd Floor
New York, NY 10019-6023
Tel: (212) 336-8330
Fax: (212) 336-8340
bcarmody@susmangodfrey.com
srabin@susmangodfrey.com
sshepard@susmangodfrey.com

Michael F. Ram
MORGAN & MORGAN
711 Van Ness Ave., Suite 500
San Francisco, CA 94102
Tel: (415) 358-6913
Fax: (415) 358-6923
mram@forthepeople.com

John A. Yanchunis (*Pro Hac Vice*)
Ryan J. McGee (*Pro Hac Vice*)
MORGAN & MORGAN
201 N. Franklin Street, 7th Floor
Tampa, FL 33602
Tel: (813) 223-5505
Fax: (813) 222-4736
jyanchunis@forthepeople.com
rmcgee@forthepeople.com

Attorneys for Plaintiffs
CHASOM BROWN, MARIA NGUYEN, WILLIAM BYATT,
JEREMY DAVIS, and CHRISTOPHER CASTILLO

Andrew H. Schapiro (*Pro Hac Vice*)
QUINN EMANUEL URQUHART &
SULLIVAN, LLP
191 N. Wacker Drive, Suite 2700
Chicago, IL 60606
Tel: (312) 705-7400
Fax: (312) 705-7401
andrewschapiro@quinnemanuel.com

Jonathan Tse
QUINN EMANUEL URQUHART &
SULLIVAN, LLP
50 California Street, 22nd Floor
San Francisco, CA 94111
Tel: (415) 875-6600
Fax: (415) 875-6700
jonathantse@quinnemanuel.com

Stephen A. Broome
Viola Trebicka
QUINN EMANUEL URQUHART &
SULLIVAN, LLP
865 S. Figueroa Street; 10th Floor
Los Angeles, CA 90017
Tel: (213) 443-3000
Fax: (213) 443-3100
stephenbroome@quinnemanuel.com
violatrebicka@quinnemanuel.com

Diane M. Doolittle
Thao Thai
QUINN EMANUEL URQUHART &
SULLIVAN, LLP
555 Twin Dolphin Drive, 5th Floor
Redwood Shores, CA 94065
Tel: (650) 801-5000
Fax: (650) 801-5100
dianedoolittle@quinnemanuel.com
thaothai@quinnemanuel.com

William Burck (*Pro Hac Vice*)
Josef Ansorge (*Pro Hac Vice*)
QUINN EMANUEL URQUHART &
SULLIVAN, LLP
1300 I Street NW, Suite 900
Washington, D.C., 20005
Tel: (202) 538-8000
Fax: (202) 538-8100
williamburck@quinnemanuel.com
josefansorge@quinnemanuel.com

Attorneys for Defendant
GOOGLE LLC

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on August 27, 2021, at San Francisco, California.


Mary Ann Rubalcaba

EXHIBIT 45



Via Email Delivery
September 20, 2021

Ryan J. McGee
MORGAN & MORGAN
201 N. Franklin Street
Tampa, FL - Florida 33602

Re: CHASOM BROWN, et al. v. GOOGLE, LLC

Dear Counsel,

I am writing on behalf of Apple Inc. ("Apple") with regard to the subpoena in the above-referenced matter. This subpoena was received at Apple on August 13, 2021. After completing a review, Apple responds on the following grounds:

(1) Apple is not in possession of the requested records

Apple does maintain documents sufficient to "IDENTIFY all individuals who have used a Private Window or Private Browsing mode in Safari..." and therefore has no documents to provide.

Through correspondence by this letter, Apple does not intend to waive any other applicable objections, including personal jurisdiction.

Sincerely,

A handwritten signature in dark ink, appearing to read "Sean Pinner", is located below the "Sincerely," text.

Sean Pinner
Corporate Counsel
Privacy & Law Enforcement Compliance
Apple Inc.
One Apple Park Way
105-2CLP
Cupertino, CA 95014
<http://www.apple.com/privacy/>
<https://www.apple.com/privacy/docs/legal-process-guidelines-us.pdf>

EXHIBIT 46

EMILY JOHNSON HENN (Bar No. 269482)
KATHRYN E. CAHOY (Bar No. 298777)
COVINGTON & BURLING LLP
3000 El Camino Real
5 Palo Alto Square, 10th Floor
Palo Alto, CA 94306-2112
Telephone: + 1 (650) 632-4700
Facsimile: + 1 (650) 632-4800
Email: ehenn@cov.com
Email: kcahoy@cov.com

JENNA L. ZHANG (Bar No. 336105)
COVINGTON & BURLING LLP
Salesforce Tower
415 Mission Street, Suite 5400
San Francisco, CA 94105-2533
Telephone: + 1 (415) 591-6000
Facsimile: + 1 (415) 591-6091
Email: jzhang@cov.com

*Attorneys for Third-Party Respondent
Microsoft Corporation*

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

CHASOM BROWN, MARIA NGUYEN,
WILLIAM BYATT, JEREMY DAVIS, and
CHRISTOPHER CASTILLO, individually and on
behalf of all others similarly situated,

Plaintiffs,

v.

GOOGLE LLC,

Defendant.

Civil Case No. 5:20-cv-03664-LHK

**THIRD-PARTY RESPONDENT
MICROSOFT CORPORATION'S
OBJECTIONS AND RESPONSES TO
PLAINTIFFS' SUBPOENA**

1 Pursuant to Rule 45 of the Federal Rules of Civil Procedure, Third-Party Respondent Microsoft
2 Corporation, by and through undersigned counsel, submits the following objections and response to
3 Plaintiffs Chasom Brown et al.'s Subpoena to Produce Documents.

4 **RESERVATION OF RIGHTS**

5 Microsoft responds to the Subpoena to the best of its knowledge at the present time and reserves
6 the right at any time to supplement, amend, correct, or clarify its responses and objections, but
7 undertakes no obligation to do so beyond the obligations imposed by the Federal Rules of Civil
8 Procedure, the Local Rules of this Court, and other applicable orders or rules. Any supplemental or
9 amended response shall not function as a waiver of any privilege or objection Microsoft has or may
10 assert. Any response to the Subpoena or a production of documents or things made by Microsoft will be
11 solely for the purpose of this action, without waiving or intending to waive, but, on the contrary,
12 preserving and intending to preserve: (a) the right to object on any grounds, at any time, to other
13 discovery requests relating to the subject of the Subpoena to which Microsoft has responded; (b) the
14 right to object, on the grounds of competency, privilege, relevancy, materiality, confidentiality,
15 authenticity, admissibility, or any other proper grounds, to the use of the responses, documents, or
16 information provided by Microsoft as evidence for any purpose, in whole or in part, in any subsequent
17 proceeding, or in any trial in this action or any other action; and (c) the right at any time to revise,
18 correct, supplement, or clarify Microsoft's responses or objections. That Microsoft has objected or
19 responded to the Subpoena is not and should not be taken as an admission that Microsoft accepts or
20 admits the existence of any fact set forth in or assumed by the Subpoena, or as an indication that
21 Microsoft agrees with or adopts any characterization or statement within the Subpoena.

22 **OBJECTIONS TO PLAINTIFFS' DEFINITIONS & INSTRUCTIONS**

23 1. Microsoft objects to the "Definitions" and "Instructions" to the extent they seek to
24 impose obligations beyond or inconsistent with those imposed by the Federal Rules of Civil Procedure,
25 the Local Rules of this Court, and/or the terms of the Stipulated Protective Order between Plaintiffs and
26 Defendant Google LLC, or between any parties to the above-captioned action.
27
28

2. Microsoft objects to Definition A (Definition of “All”) and Instruction 1(c) as overly broad and unduly burdensome because they seek to require Microsoft to produce “any and all” of the requested material, which courts consistently agree is “overbroad and impermissible.” *Henry v. Morgan’s Hotel Grp., Inc.*, 2016 WL 303114, at *2 (S.D.N.Y. Jan. 25, 2016) (“Blanket requests of this kind are plainly overbroad and impermissible.”); *Belling v. DDP Holdings, Inc.*, 2013 WL 12140986, at *3 (C.D. Cal. May 30, 2013) (“blanket requests” for “any and all documents” are “overbroad on their face”).

3. Microsoft objects to Definition B (Definition of “Document”) to the extent the definition goes beyond or is inconsistent with the definition in Fed. R. Civ. P. 34. Microsoft will interpret “Document” as defined in the Rule 34.

4. Microsoft objects to Definition C (Definition of “Identify”) as unduly burdensome and disproportionate to the extent that the listed categories of information cannot be associated with or linked to a specific individual or Google user.

5. Microsoft objects to Definition D (Definition of “You” and “Your”) on the grounds of overbreadth, undue burden, and proportionality, and as seeking privileged information, to the extent it seeks information outside the possession, custody, or control of Microsoft through references to “attorneys, agents, representatives, predecessors, successors, assigns, and anyone acting or purporting to act on [Microsoft’s] behalf.” Microsoft will interpret “You” and “Your” to mean the third-party respondent, Microsoft Corporation.

6. Microsoft objects to Instructions 10–12 as overbroad, unduly burdensome, and not proportional to the needs of the case to the extent they purport to seek information not in Microsoft’s possession, custody, or control.

DOCUMENT REQUEST

REQUEST FOR PRODUCTION NO. 1

ALL DOCUMENTS sufficient to IDENTIFY all individuals who have used InPrivate Browsing mode in Microsoft IE/Edge from June 1, 2016 to the present.

RESPONSE TO REQUEST FOR PRODUCTION NO. 1

Microsoft objects to this Request because it calls for the disclosure of information that, if available at all, is sensitive, confidential, or proprietary information, or information protected by the right to privacy for which no such substantial need has been demonstrated. Microsoft further objects to this Request as overbroad, unduly burdensome, and not proportional to the needs of the case because it seeks information (the identity of members of a putative class) that, if available at all, should be sought from parties to the litigation. Microsoft further objects to this Request as overbroad, unduly burdensome, not proportional to the needs of the case, and not likely to lead to the discovery of relevant evidence because it seeks information that, if available at all, has no apparent relation to the claims in the case or the class plaintiff seeks to certify. Microsoft further objects to this Request as overly broad, unduly burdensome, not proportional to the needs of the case, not likely to lead to the discovery of relevant evidence, and as seeking information that is not reasonably accessible, to the extent it purports to require Microsoft to create documents that do not otherwise exist. Microsoft further objects to this Request to the extent it calls for the production of data or information in a form that is not maintained and readily accessible in the usual course of business.

Based on these objections, and based on its investigation to date, Microsoft responds it does not have documents responsive to the Request. Microsoft will supplement this response if necessary as its investigation proceeds.

Dated: August 27, 2021

COVINGTON & BURLING LLP

By: /s/ Emily Johnson Henn
 EMILY JOHNSON HENN (Bar No. 269482)
 KATHRYN E. CAHOY (Bar No. 298777)
 COVINGTON & BURLING LLP
 3000 El Camino Real
 5 Palo Alto Square, 10th Floor
 Palo Alto, CA 94306-2112
 Telephone: + 1 (650) 632-4700
 Facsimile: + 1 (650) 632-4800
 Email: ehenn@cov.com
 Email: kcahoy@cov.com

JENNA L. ZHANG (SBN 336105)
COVINGTON & BURLING LLP
Salesforce Tower
415 Mission Street, Suite 5400
San Francisco, CA 94105-2533
Telephone: + 1 (415) 591-6000
Facsimile: + 1 (415) 591-6091
Email: jzhang@cov.com

*Attorneys for Third-Party Respondent
Microsoft Corporation*

PROOF OF SERVICE

I declare that I am an attorney with the law firm of Covington & Burling LLP, whose address is Salesforce Tower 415 Mission Street, Suite 5400 San Francisco, CA 94105-2533. I am over the age of eighteen years and not a party to this action. On August 27 2021, I caused a true and correct copy of the foregoing document to be served on counsel for plaintiff in this action via electronic mail addressed as follows:

BOIES SCHILLER FLEXNER LLP Mark C. Mao mmao@bsflp.com Sean P. Rodriguez srodriguez@bsflp.com Beko Richardson brichardson@bsflp.com James Lee jlee@bsflp.com Rossana Baeza rbaeza@bsflp.com	SUSMAN GODFREY L.L.P. Amanda K. Bonn abonn@susmangodfrey.com William S. Carmody bcarmody@susmangodfrey.com Shawn Rabin srabin@susmangodfrey.com Steven M. Shepard sshepard@susmangodfrey.com
MORGAN & MORGAN Michael F. Ram mram@forthepeople.com John A. Yanchunis jyanchunis@forthepeople.com Ryan J. McGee rmcgee@forthepeople.com Marie Appel mappel@forthepeople.com	

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

DATED: August 27, 2021

By: /s/ Jenna L. Zhang
Jenna L. Zhang

EXHIBIT 47
Redacted Version of
Document Sought to
be Sealed

CHASOM BROWN, ET AL. vs GOOGLE, LLC, ET AL.
Hearing on 03/23/2022

1

2

UNITED STATES DISTRICT COURT

3

NORTHERN DISTRICT OF CALIFORNIA

4

CASE NO.: 4:20-03664-YGR-AVK

5

6 CHASOM BROWN, MARIA NGUYEN and

7 WILLIAM BYATT, individually and on

8 Behalf of all other similarly situated,

9

Plaintiffs,

10 v.

11 GOOGLE, LLC and ALPHABET, INC.,

12

Defendants.

13

14

15

16

HEARING

17

18

19

HEARING BEFORE: Special Master Douglas Brush

20

DATE TAKEN: Wednesday, March 23rd, 2022

21

TIME: Unknown

22

TAKEN: Remotely via Zoom

23

24

25

TRANSCRIBED BY: KIMBERLY H. NOLAN

CHASOM BROWN, ET AL. vs GOOGLE, LLC, ET AL.
Hearing on 03/23/2022

Page 2

1 A P P E A R A N C E S

2

3 For the Plaintiffs:

4 MARK C. MAO, ESQUIRE

5 Boies, Schiller & Flexner, LLP

6 44 Montgomery Street, 41st Floor

7 San Francisco, California 94104

8 415.293.6800

9

10 For Defendant Google, LLC:

11 ANDREW H. SCHAPIRO, ESQUIRE

12 Quinn, Emanuel, Urquhart & Sullivan, LLP

13 191 North Wacker Drive, Suite 2700

14 Chicago, Illinois 60606

15 312.705.7403

16

17 For Defendant Google, LLC:

18 JOSEF ANSORGE, ESQUIRE

19 Quinn, Emanuel, Urquhart & Sullivan, LLP

20 1300 L Street Northwest, Suite 900

21 Washington, D.C. 20005

22 202.538.8000

23

24 Also Present:

25 Tracy Gao, Law Clerk at Quinn, Emanuel, Urquhart & Sullivan

CHASOM BROWN, ET AL. vs GOOGLE, LLC, ET AL.
Hearing on 03/23/2022

Page 40

1 when proceeding with the proto as a unit of analysis, or
2 maybe even the field as a unit of analysis, is it's still
3 tied to a very specific log source in this case.

4 So, there are specific [REDACTED] logs that we've
5 disclosed to you that have the field that's written, that
6 actually have that value. If that's a search you're
7 requesting, we can figure out whether those entail publisher
8 data.

9 But I want to clarify that because something is in
10 a proto, that does not mean it's in every log that uses that
11 proto. The proto is a list of all potential things that
12 could be filled in.

13 A lot of those are access-restricted, can only be
14 filled in by specific logs, and it's for that reason that in
15 our preservation proposal what we have tried to do is move
16 from the log level of analysis into the field level, where
17 if we agree these are the key fields that you're interested
18 in, we will work to figure out what is the longest period of
19 log where that exists.

20 That's separate from us changing the preserved --
21 preservation for entire log infrastructures, and I think
22 it's the most efficient way for us to proceed.

23 MR. MAO: But that field is already in [REDACTED] of
24 the logs in which -- in [REDACTED] of the [REDACTED] Young logs --
25 right? -- and that's on the ad side, that's not on the

CHASOM BROWN, ET AL. vs GOOGLE, LLC, ET AL.
Hearing on 03/23/2022

Page 41

1 [REDACTED] side. In my understanding from Dr. Sadowski's
2 deposition, that field had been constructed and had existed
3 ever since [REDACTED]

4 MR. ANSORGE: And, so, because a field is seen in
5 a proto and the log uses that proto, that does not mean that
6 that particular field has a value.

7 The default will be false for values, and you're
8 going to find that -- you know, it -- UMA uses a GWIS proto
9 for parts of its infrastructure. That doesn't mean that it
10 has that field written into it.

11 So, it's a -- if we need to search for information
12 related to that specific field, the special master thinks
13 that's, you know, proportional and appropriate for us to
14 proceed, I think we would -- could only do it in the
15 specific [REDACTED] logs, except if you're just looking for some
16 kind of description of the field infrastructure overall.

17 But the overall point I'm trying to make is that
18 the level of analysis -- and this is what I tried to argue
19 at our in-person hearing, too, and I'm sorry if I wasn't
20 effective in communicating it -- but I think the most
21 efficient and effective level of analysis for us is the
22 actual field and not the log infrastructure as we're
23 discussing the preservation plan, because we very quickly
24 find ourselves in a scenario where -- right? -- each log
25 will have standard preservation periods, each field will

CHASOM BROWN, ET AL. vs GOOGLE, LLC, ET AL.
Hearing on 03/23/2022

Page 42

1 have different ones.

2 But what we really need to be focused on are these
3 are the fields Plaintiffs care about, that they know about,
4 that they're focused on, that are in their complaint, and
5 for those we can figure out preservation proposals, and
6 that's what we tried to do in the proposal that we sent you.

7 MR. MAO: And I'm not trying to lock you down
8 on the logic or the structure -- right? -- I'm literally
9 saying that for the logs you have identified as part of the
10 special master process, one, what logs actually include that
11 field, whether at a proto level or at the actual log level,
12 and then, two, which of those logs actually has that
13 specific field filled. I realize that there may be --

14 SPECIAL MASTER BRUSH: (Interposing) Well, there's
15 one nuance -- you're so close. I think there's one nuance.
16 The problem is which logs have the capability for that
17 proto, because, again, I think what Mr. Ansorge is saying is
18 like just because it can doesn't mean it does exist, and
19 that's where there's this kind of ephemeral thing. And, so,
20 that map -- and so -- and, honestly, I mean -- and maybe --
21 I don't know what that is, so I'm gonna kick it back to Mr.
22 Ansorge on what that is. No.

23 Is that even a doable thing to say, okay, with the
24 logs that have been identified as part of this process,
25 which ones could have -- could potentially have that field

CHASOM BROWN, ET AL. vs GOOGLE, LLC, ET AL.
Hearing on 03/23/2022

Page 47

1 MR. ANSORGE: Okay. Well, in that case I
2 (inaudible) --

3 MR. MAO: (Interposing) I'm not saying that
4 she said under oath that she needs to go back to talk to
5 engineers to figure that out.

6 MR. ANSORGE: Well, then I think -- I would like
7 you to send us that specific quote and passage where she
8 said that she's not -- is not providing an answer.

9 Not only did she identify the specific log sources,
10 we put them on a piece of paper for you so that there'd be
11 no typo, so there'd be absolute clarity on which exist.

12 She explained when they were written and she
13 explained, most importantly, the logic by which they were
14 written, and that logic is one that we have discussed ad
15 infinitum, both before the special master and in other
16 processes, at least since July.

17 There's been 30(b)(b) corporate testimony about the
18 false positives, false negatives associated with the absence
19 of the "X" Klein data header.

20 MR. MAO: Well, look, we're not arguing the
21 merits of the case right now, we're simply trying to isolate
22 the data, the relevant data. Right?

23 My point is this popped up in the schema for [REDACTED] of
24 the [REDACTED] logs, and I'm simply asking you whether or not
25 you need to update the rest of the logs to either reflect

CHASOM BROWN, ET AL. vs GOOGLE, LLC, ET AL.
Hearing on 03/23/2022

Page 48

1 that's similarly in there -- okay? -- or that it could be in
2 there, or something else. Like you've given no explanation
3 or logic to that.

4 And by the way, Dr. Sadowski's deposition,
5 actually, the incongruence is that she didn't point to
6 either of those [REDACTED] logs which ended up showing that field.

7 So how do I reconcile you saying that this field --
8 that the logs -- the [REDACTED] logs she identified is exhaustive
9 when she didn't even list the [REDACTED] additional logs that was
10 produced as part of the special master process which did use
11 that field?

12 MR. ANSORGE: Yeah.

13 MR. MAO: How do I reconcile that?

14 MR. ANSORGE: I think you reconcile that by
15 understanding what we've been trying to explain about protos
16 since October.

17 MS. GAO: Mr. Mao, let me try to explain this.
18 So, [REDACTED] of the [REDACTED] logs, as you see, have this field, but
19 they will always be written as false because that's the
20 default written -- default writing of these logs, because
21 they don't really have the capability to write in the logs.

22 So, even if you select the sources and we run the
23 searches, all of the results you will see will be false.

24 MR. MAO: So, I think you're wrong there, Ms.
25 Gao, because I think you used the word "capability," and

CHASOM BROWN, ET AL. vs GOOGLE, LLC, ET AL.
Hearing on 03/23/2022**Page 49**

1 that's not true. I mean, it clearly has the capability to
2 do that. And the two questions are, one --

3 SPECIAL MASTER BRUSH: Well, let me pause you right
4 there, Mr. Mao, because I think there's a slight -- it's not
5 a universal capability to try to report it on, it's not --
6 even the option's not (blip) in every data source. You
7 know, there's a nuance there.

8 MR. MAO: Right. And, Mr. Brush --

9 SPECIAL MASTER BRUSH: So, what -- I guess let's
10 close this out, because we're at time. So --
11 (Speaking simultaneously)

12 MR. MAO: I'm just trying to figure that out,
13 Mr. Brush.

14 SPECIAL MASTER BRUSH: No, no, no. I understand
15 that.

16 MR. MAO: Exactly what (inaudible).

17 SPECIAL MASTER BRUSH: Yeah. It sounds like there
18 was a lot of information that was provided around this
19 topic, and if there's gaps, by all means.

20 I mean, I'm not saying we don't, but you're not
21 being -- we're not being very productive here getting to the
22 bottom of that.

23 But, you know, are you asking -- and can we do this
24 as kind of an approach -- out of the additional -- out of
25 all the identified logs in the process, is it -- what would

CHASOM BROWN, ET AL. vs GOOGLE, LLC, ET AL.
Hearing on 03/23/2022

Page 54

1 CERTIFICATION PAGE

2

3 I, Kimberly H. Nolan, Transcriptionist,
4 do hereby certify that this transcript
5 is a true and accurate record of the
6 electronically recorded proceedings,
7 transcribed by me this 1st day of
8 April, 2022.

9

10

11

12 KIMBERLY H. NOLAN

13

14

15

16

17

18

19

20

21

22

23

24

25

EXHIBIT 48

Mark C. Mao, CA Bar No. 236165
 Sean P. Rodriguez, CA Bar No. 262437
 Beko Richardson, CA Bar No. 238027
BOIES SCHILLER FLEXNER LLP
 44 Montgomery St., 41st Floor
 San Francisco, CA 94104
 Tel.: (415) 293-6800
 Fax: (415) 293-6899
 mmao@bsfllp.com
 srodriguez@bsfllp.com
 brichardson@bsfllp.com

James Lee (admitted *pro hac vice*)
 Rossana Baeza (admitted *pro hac vice*)
BOIES SCHILLER FLEXNER LLP
 100 SE 2nd St., 28th Floor
 Miami, FL 33131
 Tel.: (305) 539-8400
 Fax: (303) 539-1307
 jlee@bsfllp.com
 rbaeza@bsfllp.com

Amanda K. Bonn, CA Bar No. 270891
SUSMAN GODFREY L.L.P.
 1900 Avenue of the Stars, Suite 1400
 Los Angeles, CA. 90067
 Tel: (310) 789-3100
 Fax: (310) 789-3150
 abonn@susmangodfrey.com

Attorneys for Plaintiffs

**UNITED STATES DISTRICT COURT
 NORTHERN DISTRICT OF CALIFORNIA
 SAN JOSE DIVISION**

CHASOM BROWN, MARIA NGUYEN,
 WILLIAM BYATT, JEREMY DAVIS, and
 CHRISTOPHER CASTILLO, individually and
 on behalf of all other similarly situated,

Plaintiffs,

v.

GOOGLE LLC,

Defendant.

William S. Carmody (admitted *pro hac vice*)
 Shawn Rabin (admitted *pro hac vice*)
 Steven M. Shepard (admitted *pro hac vice*)
SUSMAN GODFREY L.L.P.
 1301 Avenue of the Americas, 32nd Floor
 New York, NY 10019-6023
 Tel.: (212) 336-8330
 Fax: (212) 336-8340
 bcarmody@susmangodfrey.com
 srabin@susmangodfrey.com
 sshepard@susmangodfrey.com

John A. Yanchunis (admitted *pro hac vice*)
 Ryan J. McGee (admitted *pro hac vice*)
MORGAN & MORGAN
 201 N. Franklin Street, 7th Floor
 Tampa, FL 33602
 Tel.: (813) 223-5505
 jyanchunis@forthepeople.com
 rmcgee@forthepeople.com

Case No. 5:20-cv-03664-LHK

**PLAINTIFFS' REQUESTS FOR
 PRODUCTION OF DOCUMENTS TO
 DEFENDANT GOOGLE LLC,
 SET TWO**

f. Profit.

REQUEST FOR PRODUCTION NO. 116:

All planning documents (e.g., business plans, marketing plans, sales plans, capital expenditure plans) related to Google's collection and/or use of class member data.

REQUEST FOR PRODUCTION NO. 117:

Documents, studies, reports, and articles that describe or pertain to the market for user data, including class member data.

REQUEST FOR PRODUCTION NO. 118:

Documents sufficient to understand how Google determines compensation for tracking user's data related to but not limited to how Google determines compensation for participants in the "Google Screenwise Trends" program.

REQUEST FOR PRODUCTION NO. 119:

Documents sufficient to identify, during the Class Period, web browser communications that did not contain any cookies.

REQUEST FOR PRODUCTION NO. 120:

Documents sufficient to identify, during the Class Period, Chrome web browser communications that did not contain any X-Client Data Header.

REQUEST FOR PRODUCTION NO. 121:

Documents sufficient to show usage data regarding the number of times Incognito sessions have been initiated during the Class Period, broken down by month.

REQUEST FOR PRODUCTION NO. 122:

Documents concerning any usage analytics regarding any Chrome browser features, including any analysis and findings regarding consumers' use of Incognito mode.

REQUEST FOR PRODUCTION NO. 123:

Documents concerning any usage analytics regarding any non-Chrome browser features, including any analysis and findings regarding consumers' use of private browsing mode on any non-Chrome browser.

REQUEST FOR PRODUCTION NO. 148:

Documents sufficient to identify all instances where Google shared any data collected in connection with any users' activity while in a private browsing mode, such as in response to any law enforcement or other request.

REQUEST FOR PRODUCTION NO. 149:

To the extent Google's response to any request for admissions served by Plaintiffs in this action is anything other than an unqualified admission, documents concerning that matter at issue with each such request for admission.

Dated: October 19, 2020

BOIES SCHILLER FLEXNER LLP

By: 
Mark C. Mao

Mark C. Mao, CA Bar No. 236165
Sean P. Rodriguez, CA Bar No. 262437
Beko Richardson, CA Bar No. 238027
BOIES SCHILLER FLEXNER LLP
44 Montgomery St., 41st Floor
San Francisco, CA 94104
Tel.: (415) 293-6800
Fax: (415) 293-6899
mmao@bsfllp.com
srodriguez@bsfllp.com
brichardson@bsfllp.com

James Lee (admitted *pro hac vice*)
Rossana Baeza (admitted *pro hac vice*)
BOIES SCHILLER FLEXNER LLP
100 SE 2nd St., 28th Floor
Miami, FL 33131
Tel.: (305) 539-8400
Fax: (303) 539-1307
jlee@bsfllp.com
rbaeza@bsfllp.com

Amanda K. Bonn, CA Bar No. 270891
SUSMAN GODFREY L.L.P
1900 Avenue of the Stars, Suite 1400
Los Angeles, CA. 90067

1 Tel: (310) 789-3100
2 Fax: (310) 789-3150
3 abonn@susmangodfrey.com

4 William S. Carmody (admitted *pro hac vice*)
5 Shawn Rabin (admitted *pro hac vice*)
6 Steven M. Shepard (admitted *pro hac vice*)
7 **SUSMAN GODFREY L.L.P.**
8 1301 Avenue of the Americas, 32nd Floor
9 New York, NY 10019-6023
10 Tel.: (212) 336-8330
11 Fax: (212) 336-8340
12 bcarmody@susmangodfrey.com
13 srabin@susmangodfrey.com
14 sshepard@susmangodfrey.com

15 John A. Yanchunis (admitted *pro hac vice*)
16 Ryan J. McGee (admitted *pro hac vice*)
17 **MORGAN & MORGAN**
18 201 N. Franklin Street, 7th Floor
19 Tampa, FL 33602
20 Tel.: (813) 223-5505
21 jyanchunis@forthepeople.com
22 rmcgee@forthepeople.com

23 *Attorneys for Plaintiffs*

PROOF OF SERVICE

I, Vicky L. Ayala, declare:

I am a citizen of the United States and employed in the City and County of San Francisco, CA. I am over the age of 18 and not a party to the within action; my business address is 44 Montgomery St., 41st Floor, San Francisco, CA 94104.

On October 19, 2020, I served the following document(s) described as:

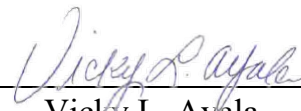
PLAINTIFFS' REQUESTS FOR PRODUCTION OF DOCUMENTS TO DEFENDANT**GOOGLE LLC, SET TWO**

- ☐ **BY FACSIMILE TRANSMISSION:** As follows: The papers have been transmitted to a facsimile machine by the person on whom it is served at the facsimile machine telephone number as last given by that person on any document which he or she has filed in the cause and served on the party making the service. The copy of the notice or other paper served by facsimile transmission shall bear a notation of the date and place of transmission and the facsimile telephone number to which transmitted or be accompanied by an unsigned copy of the affidavit or certificate of transmission which shall contain the facsimile telephone number to which the notice of other paper was transmitted to the addressee(s).
- ☐ **BY MAIL:** As follows: I am readily familiar with the firm's practice of collection and processing correspondence for mailing. Under that practice it would be deposited with U.S. postal service on that same day with postage thereon fully prepaid at San Francisco, CA, in the ordinary course of business. I am aware that on motion of the party served, service is presumed invalid if postage cancellation date or postage meter date is more than one day after date of deposit for mailing in affidavit.
- ☐ **BY OVERNIGHT MAIL:** As follows: I am readily familiar with the firm's practice of collection and processing correspondence for overnight mailing. Under that practice, it would be deposited with overnight mail on that same day prepaid at San Francisco, CA in the ordinary course of business.
- ☒ **BY ELECTRONIC MAIL TRANSMISSION:** By electronic mail transmission from vayala@bsfllp.com on October 19, 2020, by transmitting a PDF format copy of such document(s) to each such person at the e-mail address(es) listed below their address(es). The document(s) was/were transmitted by electronic transmission and such transmission was reported as complete and without error.

1 2 3 4 5	Andrew H. Schapiro (<i>pro hac vice</i>) Quinn Emanuel Urquhart & Sullivan, LLP 191 N. Wacker Drive, Suite 2700 Chicago, IL 60606 Tel: 312-705-7400 Fax: 312-705-7401 andrewschapiro@quinnemanuel.com	<i>Attorney for Defendant</i>
6 7 8 9 10	Stephen A. Broome Viola Trebicka Quinn Emanuel Urquhart & Sullivan, LLP 865 S. Figueroa Street, 10 th Floor Los Angeles, CA 90017 Tel: 213-443-3000 Fax: 213-443-3100 stephenbroome@quinnemanuel.com violatrebicka@quinnemanuel.com	<i>Attorneys for Defendant</i>
11 12 13 14 15	Diane M. Doolittle Thao Thai Quinn Emanuel Urquhart & Sullivan, LLP 555 Twin Dolphin Drive, 5 th Floor Redwood Shores, CA 94065 Tel: 650-801-5000 Fax: 650-8015100 dianedoolittle@quinnemanuel.com thaothai@quinnemanuel.com	<i>Attorneys for Defendant</i>
16 17 18 19 20	William Burck (<i>pro hac vice</i>) Josef Ansorge (<i>pro hac vice</i>) Quinn Emanuel Urquhart & Sullivan, LLP 1300 I Street NW, Suite 900 Washington, D.C., 20005 Tel: 202-538-8000 Fax: 202-538-8100 williamburck@quinnemanuel.com josefansorge@quinnemanuel.com	<i>Attorneys for Defendant</i>
21 22 23 24	Jonathan Tse Quinn Emanuel Urquhart & Sullivan, LLP 50 California Street, 22 nd Floor San Francisco, CA 94111 Tel: 415-875-6600 Fax: 415-875-6700 jonathantse@quinnemanuel.com	<i>Attorney for Defendant</i>

I declare that I am employed in the office of a member of the bar of this court at whose direction the service was made.

Executed on October 19, 2020, at San Francisco, CA.


Vicky L. Ayala

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Case No. 5:20-cv-03664-LHK

PROOF OF SERVICE

EXHIBIT 49

Redacted Version of Document Sought to be Sealed

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

- - -
CHASOM BROWN, WILLIAM : Case No.
BYATT, JEREMY DAVIS, :
CHRISTOPHER CASTILLO : 5:20-cv-03664-
and MONIQUE TRUJILLO, : LHK
individually and :
on behalf of all other :
similarly situated, : CONFIDENTIAL
:
Plaintiffs, :
:
v. :
GOOGLE, LLC, :
:
Defendant. :

- - -
Wednesday, June 16, 2021
- - -

Videotaped 30(b)(6) deposition of
GLENN BERNTSON held pursuant to notice,
beginning at 10:27 AM, on the above date,
and recorded stenographically by
Constance S. Kent, a Certified Court
Reporter, Registered Professional
Reporter and Notary Public.

* * *

MAGNA LEGAL SERVICES
(866) 624-6221
www.MagnaLS.com

1 A P P E A R A N C E S :

2 BOIES SCHILLER FLEXNER LLP
3 BY: MARK C. MAO, ESQ.
4 BEKO REBLITZ-RICHARDSON, ESQ.
5 44 Montgomery Street, 41st Floor
6 San Francisco, California 94104
7 (415) 293-6800
8 mmao@bsfllp.com
9 brichardson@bsfllp.com
10 Attorneys for Plaintiffs

11 BOIES SCHILLER FLEXNER LLP
12 BY: ROSSANA BAEZA, ESQ.
13 (pro hac vice)
14 100 SE 2nd Street, 28th Floor
15 Miami, Florida 33131
16 (305) 539-8400
17 rbaeza@bsfllp.com
18 Attorney for Plaintiffs

19 MORGAN & MORGAN
20 BY: RYAN McGEE, ESQ.
21 201 N. Franklin Street, 7th Floor
22 Tampa, Florida 33602
23 (813) 223-5505
24 rmcgee@forthepeople.com
Attorney for the Plaintiff

 SUSMAN GODFREY L.L.P
 BY: ALEXANDER FRAWLEY, ESQ.
 1900 Avenue of the Stars, Suite 1400
 Los Angeles, California 90067
 (310) 789-3100
 afrawley@susmangodfrey.com
 Attorneys for Plaintiffs

1 APPEARANCES, continued

2 QUINN EMANUEL URQUHART & SULLIVAN,
LLP

3 BY: STEPHEN BROOME, ESQUIRE
JOSEF ANSORGE, ESQUIRE

4 1300 I Street, NW, Suite 900
Washington, D.C. 20005

5 (202) 538.8000
stephenbroome@quinnemanuel.com

6 josefansorge@quinnemanuel.com
Counsel for Defendants

7

ALSO PRESENT:

8

Matthew Gubiotti, Esquire
In-house counsel for Google

9

10 Jay Bhatia

11 Chris Thompson, 233 Analytics, LLC

12 Adam Depew, Video Specialist

13 Noah Fox, Trial Technician

14

15

16

17

18

19

20

21

22

23

24

Testimony of: GLENN BERNTSON

By Mr. Mao	9
By Mr. Broome	372
By Mr. Mao	378

NO.	DESCRIPTION	PAGE
Exhibit 1	Plaintiff's Notice of 30(b)(6) Deposition	10
Exhibit 2	Confidential-Google Display Server for [REDACTED] by [REDACTED] Bates GOOG-BRWN-000029458	15
Exhibit 3	Highly Confidential-Document Entitled [REDACTED] [REDACTED] Bates GOOG-BRWN- 00078278 through 78385	107
Exhibit 4	Confidential-Document entitled [REDACTED] Bates GOOG-BRWN- 00027305 through 27313	124
Exhibit 5	Confidential-Document, http://go/[REDACTED] [REDACTED] GOOG-BRWN-00026161 through 26168	193

1 rights for what?

2 MR. MAO: I'm reserving my
3 rights to ask additional questions
4 of a witness that's properly
5 prepared to testify to the topics,
6 including the topics which the
7 court had actually ordered.

8 MR. BROOME: Okay. But you
9 don't have any more questions for
10 Mr. Berntson?

11 MR. MAO: Disagree. I don't
12 know.

13 MR. BROOME: You don't know
14 if you have any more questions for
15 him?

16 MR. MAO: Steve, stop
17 burning my time.

18 MR. BROOME: Do you have any
19 more questions for Mr. Berntson?

20 MR. MAO: I'm pausing my
21 portion.

22 MR. BROOME: Okay. I'm
23 going to take that as a no.
24 Did -- can I -- can I ask my

1 questions now? I'm going to take
2 your silence, your non-response as
3 a yes.

4 - - -

5 E X A M I N A T I O N

6 - - -

7 BY MR. BROOME:

8 Q. Mr. Berntson, do you recall
9 that Mr. Mao asked you some questions
10 today about Google mapping Biscotti IDs
11 and [REDACTED] and conversion
12 tracking?

13 A. Yes.

14 Q. And I believe you testified
15 that mapping in [REDACTED] requires a
16 Gaia ID; is that -- is that right?

17 A. That is correct.

18 Q. For the dataflow that's at
19 issue in this case where users are on
20 their browsers, they're signed out of
21 their Google accounts, they're in private
22 browsing mode, would there be any mapping
23 from Gaia to Biscotti?

24 A. No, because when you go into

1 private browsing mode, you start off with
2 a completely empty cookie jar. A
3 Biscotti is created, and if you don't
4 sign in to Google, there's no Gaia to map
5 that new Biscotti to. The Biscotti that
6 is present on the non-incognito browser
7 instance is not shared with the incognito
8 browser instance so there's no way of
9 creating that mapping from an incognito
10 session.

11 Q. Okay. And -- and conversely
12 would there be any mapping from Biscotti
13 to Gaia under those same conditions?

14 A. No. Again for similar
15 reasons, there is no Gaia to map that
16 Biscotti to.

17 Q. Mr. Mao asked -- also asked
18 you a number of questions about the
19 X-Client-Data header.

20 Do you recall that?

21 A. Yes.

22 Q. Do you understand that the
23 plaintiffs in this case have proposed
24 that Google could use the [REDACTED] [REDACTED] [REDACTED]

1 [REDACTED] [REDACTED] [REDACTED] [REDACTED]

2 [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] ?

3 A. Yes.

4 Q. And does Google use the

5 [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

6 [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] ?

7 A. [REDACTED]

8 Q. [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

9 [REDACTED] [REDACTED] [REDACTED] [REDACTED]

10 [REDACTED] [REDACTED] [REDACTED]

11 [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

12 [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

13 [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

14 [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

15 [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

16 [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

17 [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

18 [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

19 [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

20 [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

21 [REDACTED] [REDACTED]

22 [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

23 [REDACTED]

24 [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

CERTIFICATE

I HEREBY CERTIFY that the witness was duly sworn by me and that the within deposition is a true and accurate transcript of the stenographic notes of the testimony given by the witness.

It was requested before completion of the deposition that the witness, GLENN BERNTSON, have the opportunity to read and sign the deposition transcript.

Corresponding Reporter
Certified
Registered Professional Reporter
Certified LiveNote Reporter
and Notary Public
Dated: June 20, 2021



(The foregoing certification of this transcript does not apply to any reproduction of the same by any means, unless under the direct control and/or supervision of the certifying reporter.)

EXHIBIT 50
Redacted in its
Entirety

EXHIBIT 51

GOOGLE PRIVACY POLICY

When you use our services, you're trusting us with your information. We understand this is a big responsibility and work hard to protect your information and put you in control.

This Privacy Policy is meant to help you understand what information we collect, why we collect it, and how you can update, manage, export, and delete your information.

Effective October 15, 2019 | [Archived versions](#) | [Download PDF](#)

We build a range of services that help millions of people daily to explore and interact with the world in new ways. Our services include:

- Google apps, sites, and devices, like Search, YouTube, and Google Home
- Platforms like the Chrome browser and Android operating system
- Products that are integrated into third-party apps and sites, like ads and embedded Google Maps

You can use our services in a variety of ways to manage your privacy. For example, you can sign up for a Google Account if you want to create and manage content like emails and photos, or see more relevant search results. And you can use many Google services when you're signed out or without creating an account at all, like searching on Google or watching YouTube videos. You can also choose to browse the web privately using Chrome in Incognito mode. And across our services, you can adjust your privacy settings to control what we collect and how your information is used.

To help explain things as clearly as possible, we've added examples, explanatory videos, and definitions for key terms. And if you have any questions about this Privacy Policy, you can contact us.

INFORMATION GOOGLE COLLECTS

We want you to understand the types of information we collect as you use our services

We collect information to provide better services to all our users — from figuring out basic stuff like which language you speak, to more complex things like which ads you'll find most useful, the people who matter most to you online, or which YouTube videos you might like. The information Google collects, and how that information is used, depends on how you use our services and how you manage your privacy controls.

When you're not signed in to a Google Account, we store the information we collect with unique identifiers tied to the browser, application, or device you're using. This helps us do things like maintain your language preferences across browsing sessions.

When you're signed in, we also collect information that we store with your Google Account, which we treat as personal information.

Things you create or provide to us

When you create a Google Account, you provide us with personal information that includes your name and a password. You can also choose to add a phone number or payment information to your account. Even if you aren't signed in to a Google Account, you might choose to provide us with information — like an email address to receive updates about our services.

We also collect the content you create, upload, or receive from others when using our services. This includes things like email you write and receive, photos and videos you save, docs and spreadsheets you create, and comments you make on YouTube videos.

Information we collect as you use our services

Your apps, browsers & devices

We collect information about the apps, browsers, and devices you use to access Google services, which helps us provide features like automatic product updates and dimming your screen if your battery runs low.

The information we collect includes unique identifiers, browser type and settings, device type and settings, operating system, mobile network information including carrier name and phone number, and application version number. We also collect information about the interaction of your apps, browsers, and devices with our services, including IP address, crash reports, system activity, and the date, time, and referrer URL of your request.

We collect this information when a Google service on your device contacts our servers — for example, when you install an app from the Play Store or when a service checks for automatic updates. If you're using an Android device with Google apps, your device periodically contacts Google servers to provide information

about your device and connection to our services. This information includes things like your device type, carrier name, crash reports, and which apps you've installed.

Your activity

We collect information about your activity in our services, which we use to do things like recommend a YouTube video you might like. The activity information we collect may include:

- Terms you search for
- Videos you watch
- Views and interactions with content and ads
- Voice and audio information when you use audio features
- Purchase activity
- People with whom you communicate or share content
- Activity on third-party sites and apps that use our services
- Chrome browsing history you've synced with your Google Account

If you use our services to make and receive calls or send and receive messages, we may collect telephony log information like your phone number, calling-party number, receiving-party number, forwarding numbers, time and date of calls and messages, duration of calls, routing information, and types of calls.

You can visit your Google Account to find and manage activity information that's saved in your account.

[Go to Google Account](#)

Your location information

We collect information about your location when you use our services, which helps us offer features like driving directions for your weekend getaway or showtimes for movies playing near you.

Your location can be determined with varying degrees of accuracy by:

- GPS
- IP address
- Sensor data from your device
- Information about things near your device, such as Wi-Fi access points, cell towers, and Bluetooth-enabled devices

The types of location data we collect depend in part on your device and account settings. For example, you can turn your Android device's location on or off using the device's settings app. You can also turn on Location History if you want to create a private map of where you go with your signed-in devices.

In some circumstances, Google also collects information about you from publicly accessible sources. For example, if your name appears in your local newspaper, Google's Search engine may index that article and display it to other people if they search for your name. We may also collect information about you from trusted partners, including marketing partners who provide us with information about potential customers of our business services, and security partners who provide us with information to protect against abuse. We also receive information from advertisers to provide advertising and research services on their behalf.

We use various technologies to collect and store information, including cookies, pixel tags, local storage, such as browser web storage or application data caches, databases, and server logs.

WHY GOOGLE COLLECTS DATA

We use data to build better services

We use the information we collect from all our services for the following purposes:

Provide our services

We use your information to deliver our services, like processing the terms you search for in order to return results or helping you share content by suggesting recipients from your contacts.

Maintain & improve our services

We also use your information to ensure our services are working as intended, such as tracking outages or troubleshooting issues that you report to us. And we use your information to make improvements to our services — for example, understanding which search terms are most frequently misspelled helps us improve spell-check features used across our services.

Develop new services

We use the information we collect in existing services to help us develop new ones. For example, understanding how people organized their photos in Picasa, Google's first photos app, helped us design and launch Google Photos.

Provide personalized services, including content and ads

We use the information we collect to customize our services for you, including providing recommendations, personalized content, and customized search results. For example, Security Checkup provides security tips adapted to how you use Google products. And Google Play uses information like apps you've already installed and videos you've watched on YouTube to suggest new apps you might like.

Depending on your settings, we may also show you personalized ads based on your interests. For example, if you search for "mountain bikes," you may see an ad for sports equipment when you're browsing a site that shows ads served by Google. You can control what information we use to show you ads by visiting your ad settings.

- We don't show you personalized ads based on sensitive categories, such as race, religion, sexual orientation, or health.
- We don't share information that personally identifies you with advertisers, such as your name or email, unless you ask us to. For example, if you see an ad for a nearby flower shop and select the "tap to call" button, we'll connect your call and may share your phone number with the flower shop.

[Go to Ad Settings](#)

Measure performance

We use data for analytics and measurement to understand how our services are used. For example, we analyze data about your visits to our sites to do things like optimize product design. And we also use data about the ads you interact with to help advertisers understand the performance of their ad campaigns. We use a variety of tools to do this, including Google Analytics. When you visit sites that use Google Analytics, Google and a Google Analytics customer may link information about your activity from that site with activity from other sites that use our ad services.

Communicate with you

We use information we collect, like your email address, to interact with you directly. For example, we may send you a notification if we detect suspicious activity, like an attempt to sign in to your Google Account from an unusual location. Or we may let you know about upcoming changes or improvements to our services. And if you contact Google, we'll keep a record of your request in order to help solve any issues you might be facing.

Protect Google, our users, and the public

We use information to help improve the safety and reliability of our services. This includes detecting, preventing, and responding to fraud, abuse, security risks, and technical issues that could harm Google, our users, or the public.

We use different technologies to process your information for these purposes. We use automated systems that analyze your content to provide you with things like customized search results, personalized ads, or other features tailored to how you use our services. And we analyze your content to help us detect abuse such as spam, malware, and illegal content. We also use algorithms to recognize patterns in data. For example, Google Translate helps people communicate across languages by detecting common language patterns in phrases you ask it to translate.

We may combine the information we collect among our services and across your devices for the purposes described above. For example, if you watch videos of guitar players on YouTube, you might see an ad for guitar lessons on a site that uses our ad products. Depending on your account settings, your activity on

other sites and apps may be associated with your personal information in order to improve Google's services and the ads delivered by Google.

If other users already have your email address or other information that identifies you, we may show them your publicly visible Google Account information, such as your name and photo. This helps people identify an email coming from you, for example.

We'll ask for your consent before using your information for a purpose that isn't covered in this Privacy Policy.

YOUR PRIVACY CONTROLS

You have choices regarding the information we collect and how it's used

This section describes key controls for managing your privacy across our services. You can also visit the Privacy Checkup, which provides an opportunity to review and adjust important privacy settings. In addition to these tools, we also offer specific privacy settings in our products — you can learn more in our Product Privacy Guide.

[Go to Privacy Checkup](#)

Managing, reviewing, and updating your information

When you're signed in, you can always review and update information by visiting the services you use. For example, Photos and Drive are both designed to help you manage specific types of content you've saved with Google.

We also built a place for you to review and control information saved in your Google Account. Your Google Account includes:

Privacy controls

Activity Controls

Decide what types of activity you'd like saved in your account. For example, you can turn on Location History if you want traffic predictions for your daily commute, or you can save your YouTube Watch History to get better video suggestions.

[Go to Activity Controls](#)

Ad settings

Manage your preferences about the ads shown to you on Google and on sites and apps that partner with Google to show ads. You can modify your interests, choose whether your personal information is used to make ads more relevant to you, and turn on or off certain advertising services.

[Go to Ad Settings](#)

About you

Control what others see about you across Google services.

[Go to About You](#)

Shared endorsements

Choose whether your name and photo appear next to your activity, like reviews and recommendations, that appear in ads.

[Go to Shared Endorsements](#)

Information you share

If you're a G Suite user, control whom you share information with through your account on Google+.

[Go to Information You Share](#)

Ways to review & update your information

My Activity

My Activity allows you to review and control data that's created when you use Google services, like searches you've done or your visits to Google Play. You can browse by date and by topic, and delete part or all of your activity.

[Go to My Activity](#)

Google Dashboard

Google Dashboard allows you to manage information associated with specific products.

[Go to Dashboard](#)

Your personal information

Manage your contact information, such as your name, email, and phone number.

[Go to Personal Info](#)

When you're signed out, you can manage information associated with your browser or device, including:

- Signed-out search personalization: Choose whether your search activity is used to offer you more relevant results and recommendations.
- YouTube settings: Pause and delete your YouTube Search History and your YouTube Watch History.
- Ad Settings: Manage your preferences about the ads shown to you on Google and on sites and apps that partner with Google to show ads.

Exporting, removing & deleting your information

You can export a copy of content in your Google Account if you want to back it up or use it with a service outside of Google.

Export your data

You can also request to remove content from specific Google services based on applicable law.

To delete your information, you can:

- Delete your content from specific Google services
- Search for and then delete specific items from your account using My Activity
- Delete specific Google products, including your information associated with those products
- Delete your entire Google Account

Delete your information

And finally, Inactive Account Manager allows you to give someone else access to parts of your Google Account in case you're unexpectedly unable to use your account.

There are other ways to control the information Google collects whether or not you're signed in to a Google Account, including:

- Browser settings: For example, you can configure your browser to indicate when Google has set a cookie in your browser. You can also configure your browser to block all cookies from a specific domain or all domains. But remember that our services rely on cookies to function properly, for things like remembering your language preferences.
- Device-level settings: Your device may have controls that determine what information we collect. For example, you can modify location settings on your Android device.

SHARING YOUR INFORMATION

When you share your information

Many of our services let you share information with other people, and you have control over how you share. For example, you can share videos on YouTube publicly or you can decide to keep your videos private. Remember, when you share information publicly, your content may become accessible through search engines, including Google Search.

When you're signed in and interact with some Google services, like leaving comments on a YouTube video or reviewing an app in Play, your name and photo appear next to your activity. We may also display this information in ads depending on your Shared endorsements setting.

When Google shares your information

We do not share your personal information with companies, organizations, or individuals outside of Google except in the following cases:

With your consent

We'll share personal information outside of Google when we have your consent. For example, if you use Google Home to make a reservation through a booking service, we'll get your permission before sharing your name or phone number with the restaurant. We'll ask for your explicit consent to share any sensitive personal information.

With domain administrators

If you're a student or work for an organization that uses Google services (like G Suite), your domain administrator and resellers who manage your account will have access to your Google Account. They may be able to:

- Access and retain information stored in your account, like your email
- View statistics regarding your account, like how many apps you install

- Change your account password
- Suspend or terminate your account access
- Receive your account information in order to satisfy applicable law, regulation, legal process, or enforceable governmental request
- Restrict your ability to delete or edit your information or your privacy settings

For external processing

We provide personal information to our affiliates and other trusted businesses or persons to process it for us, based on our instructions and in compliance with our Privacy Policy and any other appropriate confidentiality and security measures. For example, we use service providers to help us with customer support.

For legal reasons

We will share personal information outside of Google if we have a good-faith belief that access, use, preservation, or disclosure of the information is reasonably necessary to:

- Meet any applicable law, regulation, legal process, or enforceable governmental request. We share information about the number and type of requests we receive from governments in our Transparency Report.
- Enforce applicable Terms of Service, including investigation of potential violations.
- Detect, prevent, or otherwise address fraud, security, or technical issues.
- Protect against harm to the rights, property or safety of Google, our users, or the public as required or permitted by law.

We may share non-personally identifiable information publicly and with our partners — like publishers, advertisers, developers, or rights holders. For example, we share information publicly to show trends about the general use of our services. We also allow specific partners to collect information from your browser or device for advertising and measurement purposes using their own cookies or similar technologies.

If Google is involved in a merger, acquisition, or sale of assets, we'll continue to ensure the confidentiality of your personal information and give affected users notice before personal information is transferred or becomes subject to a different privacy policy.

KEEPING YOUR INFORMATION SECURE

We build security into our services to protect your information

All Google products are built with strong security features that continuously protect your information. The insights we gain from maintaining our services help us detect and automatically block security threats from ever reaching you. And if we do detect something risky that we think you should know about, we'll notify you and help guide you through steps to stay better protected.

We work hard to protect you and Google from unauthorized access, alteration, disclosure, or destruction of information we hold, including:

- We use encryption to keep your data private while in transit
- We offer a range of security features, like Safe Browsing, Security Checkup, and 2 Step Verification to help you protect your account
- We review our information collection, storage, and processing practices, including physical security measures, to prevent unauthorized access to our systems
- We restrict access to personal information to Google employees, contractors, and agents who need that information in order to process it. Anyone with this access is subject to strict contractual confidentiality obligations and may be disciplined or terminated if they fail to meet these obligations.

EXPORTING & DELETING YOUR INFORMATION

You can export a copy of your information or delete it from your Google Account at any time

You can export a copy of content in your Google Account if you want to back it up or use it with a service outside of Google.

Export your data

To delete your information, you can:

- Delete your content from specific Google services
- Search for and then delete specific items from your account using My Activity
- Delete specific Google products, including your information associated with those products
- Delete your entire Google Account

Delete your information

Retaining your information

We retain the data we collect for different periods of time depending on what it is, how we use it, and how you configure your settings:

- Some data you can delete whenever you like, such as the content you create or upload. You can also delete activity information saved in your account, or choose to have it deleted automatically after a set period of time.
- Other data is deleted or anonymized automatically after a set period of time, such as advertising data in server logs.
- We keep some data until you delete your Google Account, such as information about how often you use our services.
- And some data we retain for longer periods of time when necessary for legitimate business or legal purposes, such as security, fraud and abuse prevention, or financial record-keeping.

When you delete data, we follow a deletion process to make sure that your data is safely and completely removed from our servers or retained only in anonymized form. We try to ensure that our services protect information from accidental or malicious deletion. Because of this, there may be delays between when you delete something and when copies are deleted from our active and backup systems.

You can read more about Google's data retention periods, including how long it takes us to delete your information.

COMPLIANCE & COOPERATION WITH REGULATORS

We regularly review this Privacy Policy and make sure that we process your information in ways that comply with it.

Data transfers

We maintain servers around the world and your information may be processed on servers located outside of the country where you live. Data protection laws vary among countries, with some providing more protection than others. Regardless of where your information is processed, we apply the same protections described in this policy. We also comply with certain legal frameworks relating to the transfer of data, such as the EU-US and Swiss-US Privacy Shield Frameworks.

When we receive formal written complaints, we respond by contacting the person who made the complaint. We work with the appropriate regulatory authorities, including local data protection authorities, to resolve any complaints regarding the transfer of your data that we cannot resolve with you directly.

ABOUT THIS POLICY

When this policy applies

This Privacy Policy applies to all of the services offered by Google LLC and its affiliates, including YouTube, Android, and services offered on third-party sites, such as advertising services. This Privacy Policy doesn't apply to services that have separate privacy policies that do not incorporate this Privacy Policy.

This Privacy Policy doesn't apply to:

- The information practices of other companies and organizations that advertise our services
- Services offered by other companies or individuals, including products or sites that may include Google services, be displayed to you in search results, or be linked from our services

Changes to this policy

We change this Privacy Policy from time to time. We will not reduce your rights under this Privacy Policy without your explicit consent. We always indicate the date the last changes were published and we offer

access to archived versions for your review. If changes are significant, we'll provide a more prominent notice (including, for certain services, email notification of Privacy Policy changes).

RELATED PRIVACY PRACTICES

Specific Google services

The following privacy notices provide additional information about some Google services:

- [Chrome & the Chrome Operating System](#)
- [Play Books](#)
- [Payments](#)
- [Fiber](#)
- [Google Fi](#)
- [G Suite for Education](#)
- [YouTube Kids](#)
- [Google Accounts Managed with Family Link, for Children under 13 \(or applicable age in your country\)](#)
- [Voice and Audio Collection from Children's Features on the Google Assistant](#)

Other useful resources

The following links highlight useful resources for you to learn more about our practices and privacy settings.

- [Your Google Account](#) is home to many of the settings you can use to manage your account
- [Privacy Checkup](#) guides you through key privacy settings for your Google Account
- [Google's safety center](#) helps you learn more about our built-in security, privacy controls, and tools to help set digital ground rules for your family online
- [Privacy & Terms](#) provides more context regarding this Privacy Policy and our Terms of Service

- Technologies includes more information about:
 - How Google uses cookies
 - Technologies used for Advertising
 - How Google uses pattern recognition to recognize things like faces in photos
 - How Google uses information from sites or apps that use our services

ads you'll find most useful

For example, if you watch videos about baking on YouTube, you may see more ads that relate to baking as you browse the web. We also may use your IP address to determine your approximate location, so that we can serve you ads for a nearby pizza delivery service if you search for "pizza." Learn more about Google ads and why you may see particular ads.

the people who matter most to you online

For example, when you type an address in the To, Cc, or Bcc field of an email you're composing, Gmail will suggest addresses based on the people you contact most frequently.

phone number

If you add your phone number to your account, it can be used for different purposes across Google services, depending on your settings. For example, your phone number can be used to help you access your account if you forget your password, help people find and connect with you, and make the ads you see more relevant to you. Learn more

payment information

For example, if you add a credit card or other payment method to your Google Account, you can use it to buy things across our services, like apps in the Play Store. We may also ask for other information, like a business tax ID, to help process your payment. In some cases, we may also need to verify your identity and may ask you for information to do this.

We may also use payment information to verify that you meet age requirements, if, for example, you enter an incorrect birthday indicating you're not old enough to have a Google Account. [Learn more](#)

devices

For example, we can use information from your devices to help you decide which device you'd like to use to install an app or view a movie you buy from Google Play. We also use this information to help protect your account.

Android device with Google apps

Android devices with Google apps include devices sold by Google or one of our partners and include phones, cameras, vehicles, wearables, and televisions. These devices use Google Play Services and other pre-installed apps that include services like Gmail, Maps, your phone's camera and phone dialer, text-to-speech conversion, keyboard input, and security features.

Views and interactions with content and ads

For example, we collect information about views and interactions with ads so we can provide aggregated reports to advertisers, like telling them whether we served their ad on a page and whether the ad was likely seen by a viewer. We may also measure other interactions, such as how you move your mouse over an ad or if you interact with the page on which the ad appears.

synced with your Google Account

Your Chrome browsing history is only saved to your account if you've enabled Chrome synchronization with your Google Account. [Learn more](#)

services to make and receive calls or send and receive messages

Examples of these services include:

- Google Hangouts, for making domestic and international calls
- Google Voice, for making calls, sending text messages, and managing voicemail
- Google Fi, for a phone plan

Sensor data from your device

Your device may have sensors that can be used to better understand your location and movement. For example, an accelerometer can be used to determine your speed and a gyroscope to figure out your direction of travel.

Information about things near your device

If you use Google's Location services on Android, we can improve the performance of apps that rely on your location, like Google Maps. If you use Google's Location services, your device sends information to Google about its location, sensors (like accelerometer), and nearby cell towers and Wi-Fi access points (like MAC address and signal strength). All these things help to determine your location. You can use your device settings to enable Google Location services. [Learn more](#)

publicly accessible sources

For example, we may collect information that's publicly available online or from other public sources to help train Google's language models and build features like Google Translate.

protect against abuse

For example, information about security threats can help us notify you if we think your account has been compromised (at which point we can help you take steps to protect your account).

advertising and research services on their behalf

For example, advertisers may upload data from their loyalty-card programs so that they can better understand the performance of their ad campaigns. We only provide aggregated reports to advertisers that don't reveal information about individual people.

deliver our services

Examples of how we use your information to deliver our services include:

- We use the IP address assigned to your device to send you the data you requested, such as loading a YouTube video
- We use unique identifiers stored in cookies on your device to help us authenticate you as the person who should have access to your Google Account
- Photos and videos you upload to Google Photos are used to help you create albums, animations, and other creations that you can share. [Learn more](#)
- A flight confirmation email you receive may be used to create a "check-in" button that appears in your Gmail
- When you purchase services or physical goods from us, you may provide us information like your shipping address or delivery instructions. We use this information for things like processing, fulfilling, and delivering your order, and to provide support in connection with the product or service you purchase.

ensure our services are working as intended

For example, we continuously monitor our systems to look for problems. And if we find something wrong with a specific feature, reviewing activity information collected before the problem started allows us to fix things more quickly.

make improvements

For example, we use cookies to analyze how people interact with our services. And that analysis can help us build better products. For example, it may help us discover that it's taking people too long to complete a

certain task or that they have trouble finishing steps at all. We can then redesign that feature and improve the product for everyone.

customized search results

For example, when you're signed in to your Google Account and have the Web & App Activity control enabled, you can get more relevant search results that are based on your previous searches and activity from other Google services. You can learn more [here](#). You may also get customized search results even when you're signed out. If you don't want this level of search customization, you can search and browse privately or turn off signed-out search personalization.

personalized ads

You may also see personalized ads based on information from the advertiser. If you shopped on an advertiser's website, for example, they can use that visit information to show you ads. [Learn more](#)

sensitive categories

When showing you personalized ads, we use topics that we think might be of interest to you based on your activity. For example, you may see ads for things like "Cooking and Recipes" or "Air Travel." We don't use topics or show personalized ads based on sensitive categories like race, religion, sexual orientation, or health. And we require the same from advertisers that use our services.

may link information

Google Analytics relies on first-party cookies, which means the cookies are set by the Google Analytics customer. Using our systems, data generated through Google Analytics can be linked by the Google Analytics customer and by Google to third-party cookies that are related to visits to other websites. For example, an advertiser may want to use its Google Analytics data to create more relevant ads, or to further analyze its traffic. [Learn more](#)

safety and reliability

Some examples of how we use your information to help keep our services safe and reliable include:

- Collecting and analyzing IP addresses and cookie data to protect against automated abuse. This abuse takes many forms, such as sending spam to Gmail users, stealing money from advertisers by fraudulently clicking on ads, or censoring content by launching a Distributed Denial of Service (DDoS) attack.
- The “last account activity” feature in Gmail can help you find out if and when someone accessed your email without your knowledge. This feature shows you information about recent activity in Gmail, such as the IP addresses that accessed your mail, the associated location, and the date and time of access. [Learn more](#)

detect abuse

When we detect spam, malware, illegal content, and other forms of abuse on our systems in violation of our policies, we may disable your account or take other appropriate action. In certain circumstances, we may also report the violation to appropriate authorities.

combine the information we collect

Some examples of how we combine the information we collect include:

- When you’re signed in to your Google Account and search on Google, you can see search results from the public web, along with relevant information from the content you have in other Google products, like Gmail or Google Calendar. This can include things like the status of your upcoming flights, restaurant, and hotel reservations, or your photos. [Learn more](#)
- If you have communicated with someone via Gmail and want to add them to a Google Doc or an event in Google Calendar, Google makes it easy to do so by autocompleting their email address when you start to type in their name. This feature makes it easier to share things with people you know. [Learn more](#)
- The Google app can use data that you have stored in other Google products to show you personalized content, depending on your settings. For example, if you have searches stored in your Web & App Activity, the Google app can show you news articles and other information about your interests, like sports scores, based your activity. [Learn more](#)

- If you link your Google Account to your Google Home, you can manage your information and get things done through the Google Assistant. For example, you can add events to your Google Calendar or get your schedule for the day, ask for status updates on your upcoming flight, or send information like driving directions to your phone. [Learn more](#)

your activity on other sites and apps

This activity might come from your use of Google services, like from syncing your account with Chrome or your visits to sites and apps that partner with Google. Many websites and apps partner with Google to improve their content and services. For example, a website might use our advertising services (like AdSense) or analytics tools (like Google Analytics), or it might embed other content (such as videos from YouTube). These services may share information about your activity with Google and, depending on your account settings and the products in use (for instance, when a partner uses Google Analytics in conjunction with our advertising services), this data may be associated with your personal information.

[Learn more about how Google uses data when you use our partners' sites or apps.](#)

partner with Google

There are over 2 million non-Google websites and apps that partner with Google to show ads. [Learn more](#)

specific Google services

For example, you can delete your blog from Blogger or a Google Site you own from Google Sites. You can also delete reviews you've left on apps, games, and other content in the Play Store.

rely on cookies to function properly

For example, we use a cookie called 'lbcs' that makes it possible for you to open many Google Docs in one browser. Blocking this cookie would prevent Google Docs from working as expected. [Learn more](#)

legal process, or enforceable governmental request

Like other technology and communications companies, Google regularly receives requests from governments and courts around the world to disclose user data. Respect for the privacy and security of data you store with Google underpins our approach to complying with these legal requests. Our legal team reviews each and every request, regardless of type, and we frequently push back when a request appears to be overly broad or doesn't follow the correct process. Learn more in our Transparency Report.

show trends

When lots of people start searching for something, it can provide useful information about particular trends at that time. Google Trends samples Google web searches to estimate the popularity of searches over a certain period of time and shares those results publicly in aggregated terms. Learn more

specific partners

For example, we allow YouTube creators and advertisers to work with measurement companies to learn about the audience of their YouTube videos or ads, using cookies or similar technologies. Another example is merchants on our shopping pages, who use cookies to understand how many different people see their product listings. Learn more about these partners and how they use your information.

servers around the world

For example, we operate data centers located around the world to help keep our products continuously available for users.

third parties

For example, we process your information to report use statistics to rights holders about how their content was used in our services. We may also process your information if people search for your name and we display search results for sites containing publicly available information about you.

appropriate safeguards

For example, we may anonymize data, or encrypt data to ensure it can't be linked to other information about you. [Learn more](#)

ensure and improve

For example, we analyze how people interact with advertising to improve the performance of our ads.

Customizing our services

For example, we may display a Google Doodle on the Search homepage to celebrate an event specific to your country.

Affiliates

An affiliate is an entity that belongs to the Google group of companies, including the following companies that provide consumer services in the EU: Google Ireland Limited, Google Commerce Ltd, Google Payment Corp, and Google Dialer Inc. [Learn more about the companies providing business services in the EU.](#)

Algorithm

A process or set of rules followed by a computer in performing problem-solving operations.

Application data cache

An application data cache is a data repository on a device. It can, for example, enable a web application to run without an internet connection and improve the performance of the application by enabling faster loading of content.

Browser web storage

Browser web storage enables websites to store data in a browser on a device. When used in "local storage" mode, it enables data to be stored across sessions. This makes data retrievable even after a browser has been closed and reopened. One technology that facilitates web storage is HTML 5.

Cookies and similar technologies

A cookie is a small file containing a string of characters that is sent to your computer when you visit a website. When you visit the site again, the cookie allows that site to recognize your browser. Cookies may store user preferences and other information. You can configure your browser to refuse all cookies or to indicate when a cookie is being sent. However, some website features or services may not function properly without cookies. Learn more about how Google uses cookies and how Google uses data, including cookies, when you use our partners' sites or apps.

Device

A device is a computer that can be used to access Google services. For example, desktop computers, tablets, smart speakers, and smartphones are all considered devices.

Non-personally identifiable information

This is information that is recorded about users so that it no longer reflects or references an individually-identifiable user.

IP address

Every device connected to the Internet is assigned a number known as an Internet protocol (IP) address. These numbers are usually assigned in geographic blocks. An IP address can often be used to identify the location from which a device is connecting to the Internet.

Pixel tag

A pixel tag is a type of technology placed on a website or within the body of an email for the purpose of tracking certain activity, such as views of a website or when an email is opened. Pixel tags are often used in combination with cookies.

Personal information

This is information that you provide to us which personally identifies you, such as your name, email address, or billing information, or other data that can be reasonably linked to such information by Google, such as information we associate with your Google Account.

Sensitive personal information

This is a particular category of personal information relating to topics such as confidential medical facts, racial or ethnic origins, political or religious beliefs, or sexuality.

Server logs

Like most websites, our servers automatically record the page requests made when you visit our sites. These “server logs” typically include your web request, Internet Protocol address, browser type, browser language, the date and time of your request, and one or more cookies that may uniquely identify your browser.

A typical log entry for a search for “cars” looks like this:

```
123.45.67.89 - 25/Mar/2003 10:15:32 -  
http://www.google.com/search?q=cars -  
Firefox 1.0.7; Windows NT 5.1 -  
740674ce2123e969
```

- 123.45.67.89 is the Internet Protocol address assigned to the user by the user’s ISP. Depending on the user’s service, a different address may be assigned to the user by their service provider each time they connect to the Internet.
- 25/Mar/2003 10:15:32 is the date and time of the query.
- http://www.google.com/search?q=cars is the requested URL, including the search query.

- Firefox 1.0.7; Windows NT 5.1 is the browser and operating system being used.
- 740674ce2123a969 is the unique cookie ID assigned to this particular computer the first time it visited Google. (Cookies can be deleted by users. If the user has deleted the cookie from the computer since the last time they've visited Google, then it will be the unique cookie ID assigned to their device the next time they visit Google from that particular device).

Unique identifiers

A unique identifier is a string of characters that can be used to uniquely identify a browser, app, or device. Different identifiers vary in how permanent they are, whether they can be reset by users, and how they can be accessed.

Unique identifiers can be used for various purposes, including security and fraud detection, syncing services such as your email inbox, remembering your preferences, and providing personalized advertising. For example, unique identifiers stored in cookies help sites display content in your browser in your preferred language. You can configure your browser to refuse all cookies or to indicate when a cookie is being sent. [Learn more about how Google uses cookies.](#)

On other platforms besides browsers, unique identifiers are used to recognize a specific device or app on that device. For example, a unique identifier such as the Advertising ID is used to provide relevant advertising on Android devices, and can be managed in your device's settings. Unique identifiers may also be incorporated into a device by its manufacturer (sometimes called a universally unique ID or UUID), such as the IMEI-number of a mobile phone. For example, a device's unique identifier can be used to customize our service to your device or analyze device issues related to our services.